RISK MANAGEMENT 101

A Risk Management Guide for Information Security

Compiled by Muhammad Kazim

Table of Contents

Introduction

The principal goal of an organization's risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets.

Purpose

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Guide Structure

The remaining sections of this guide discuss the following:

- **Section 2** provides an overview of risk management, how it fits into the system development life cycle (SDLC), and the roles of individuals who support and use this process.
- **Section 3** describes the risk assessment methodology and the nine primary steps in conducting a risk assessment of an IT system.
- **Section 4** describes the risk mitigation process, including risk mitigation options and strategy, approach for control implementation, control categories, cost-benefit analysis, and residual risk.
- **Section 5** discusses the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.

Risk Management Overview

Importance of Risk Management

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment.

Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system.

The risk assessment methodology encompasses nine primary steps, which are

- Step 1 - System Characterization
- Step 2 - Threat Identification
- Step 3 - Vulnerability Identification
- Step 4 - Control Analysis
- Step 5 - Likelihood Determination
- Step 6 - Impact Analysis
- Step 7 - Risk Determination
- Step 8 - Control Recommendations

- Step 9 - Results Documentation.

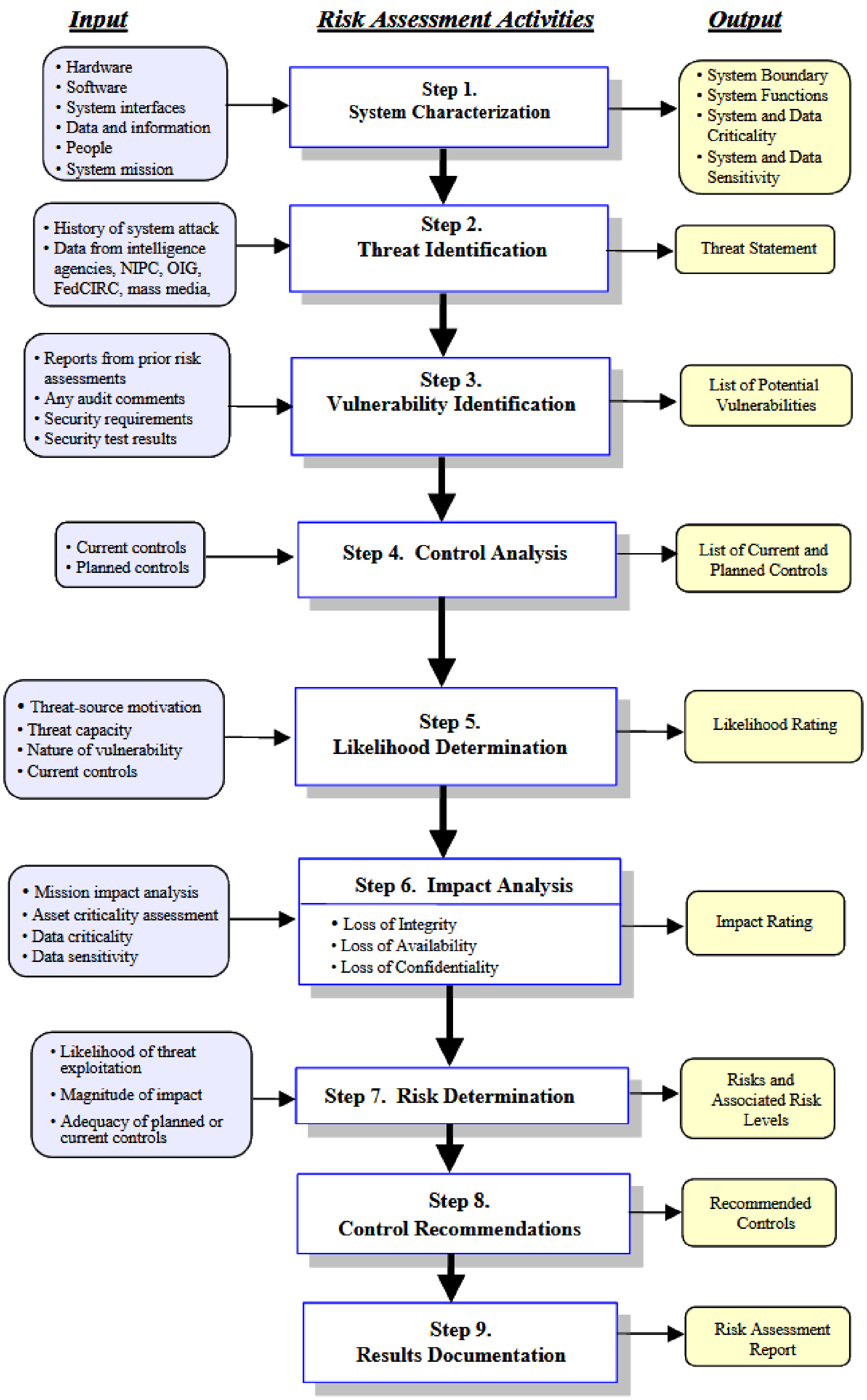


Figure 3-1. Risk Assessment Methodology Flowchart

Step – 1: System Characterization

Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

System-Related Information

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the IT system
- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.

Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:

- Users of the system
- System security policies governing the IT system
- System security architecture
- Current network topology
- Technical controls used for the IT system
- Flow of information pertaining to the IT system
- Management controls used for the IT system
- Operational controls used for the IT system
- Physical security environment of the IT system
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

Information Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

- **Questionnaire**: To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system.

- **On-site Interviews:** Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed).
- **Document Review:** Policy documents (e.g., legislative documentation, directives), system documentation.
- **Use of Automated Scanning Tool:** Proactive technical methods can be used to collect system information efficiently.

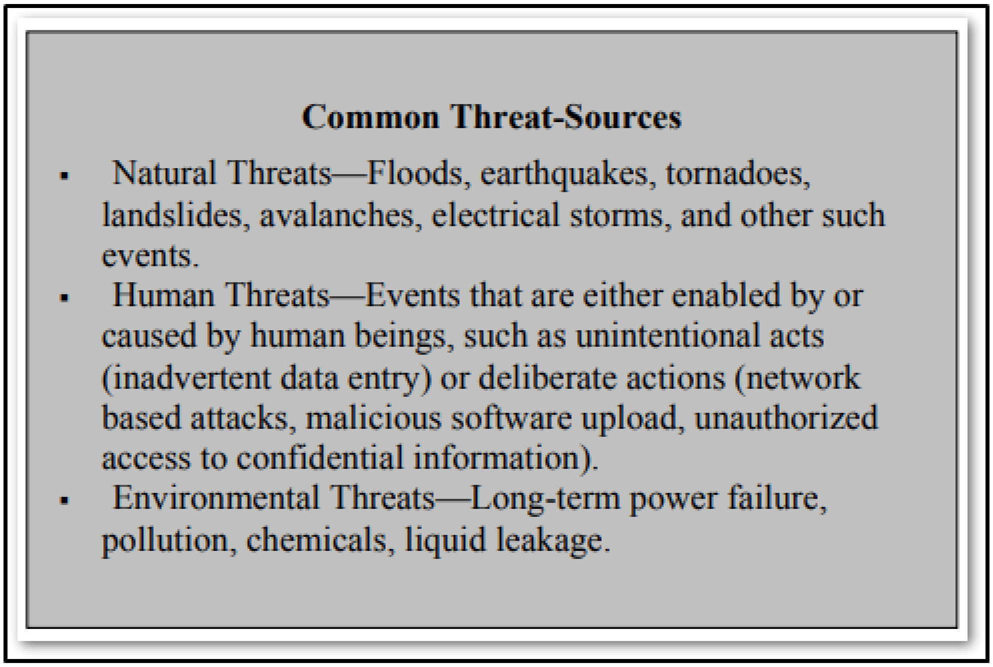
Output from Step 1 - Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary

Step – 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability.

Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat-sources can be natural, human, or environmental.



Common Threat-Sources

- Natural Threats—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- Human Threats—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 Threats—Long-term power failure, pollution, chemicals, liquid leakage.

Motivation and Threat Action

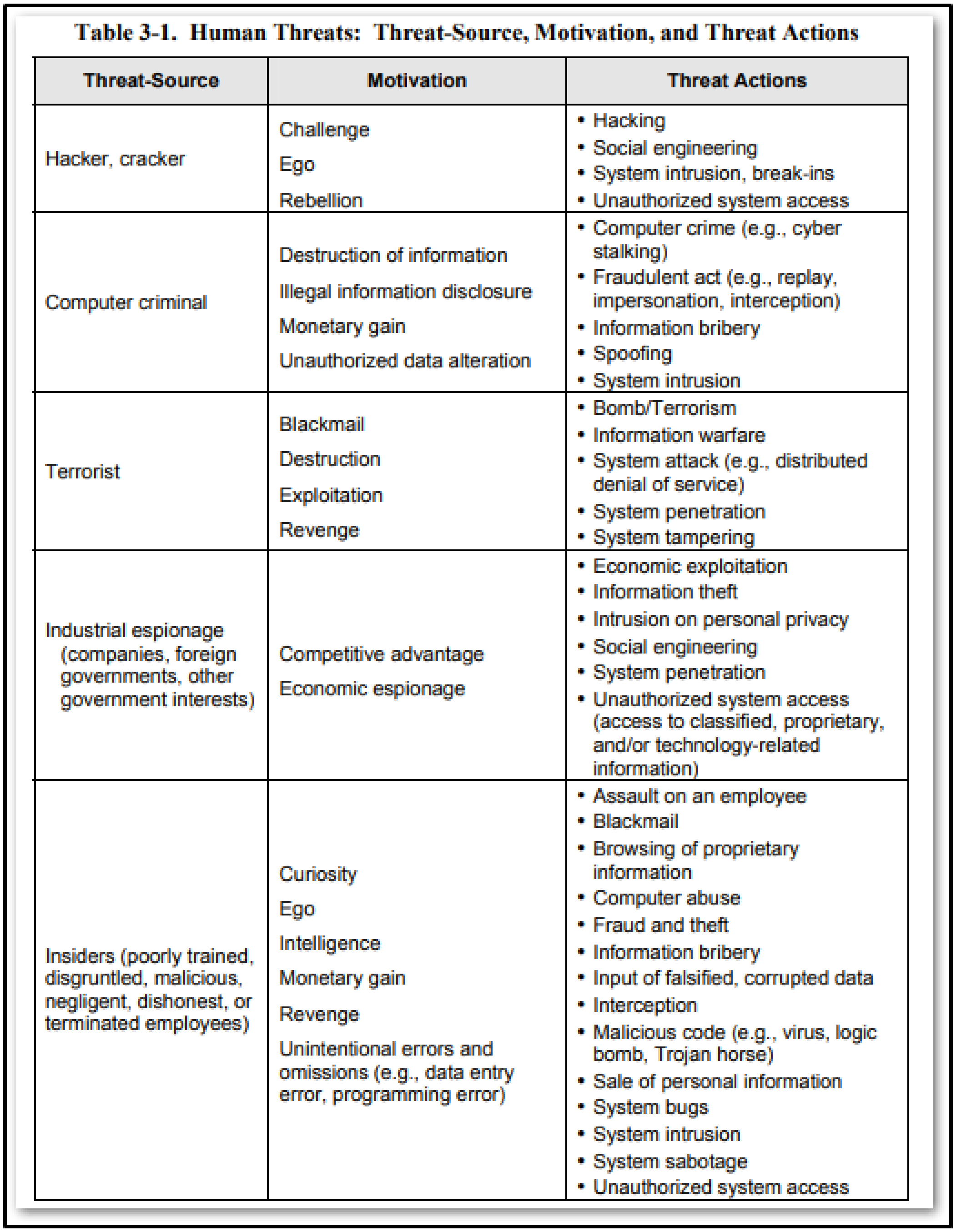


Table 3-1. Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Output from Step 2 - A threat statement containing a list of threat-sources that could exploit system vulnerabilities

Step – 3: Vulnerability Identification

The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

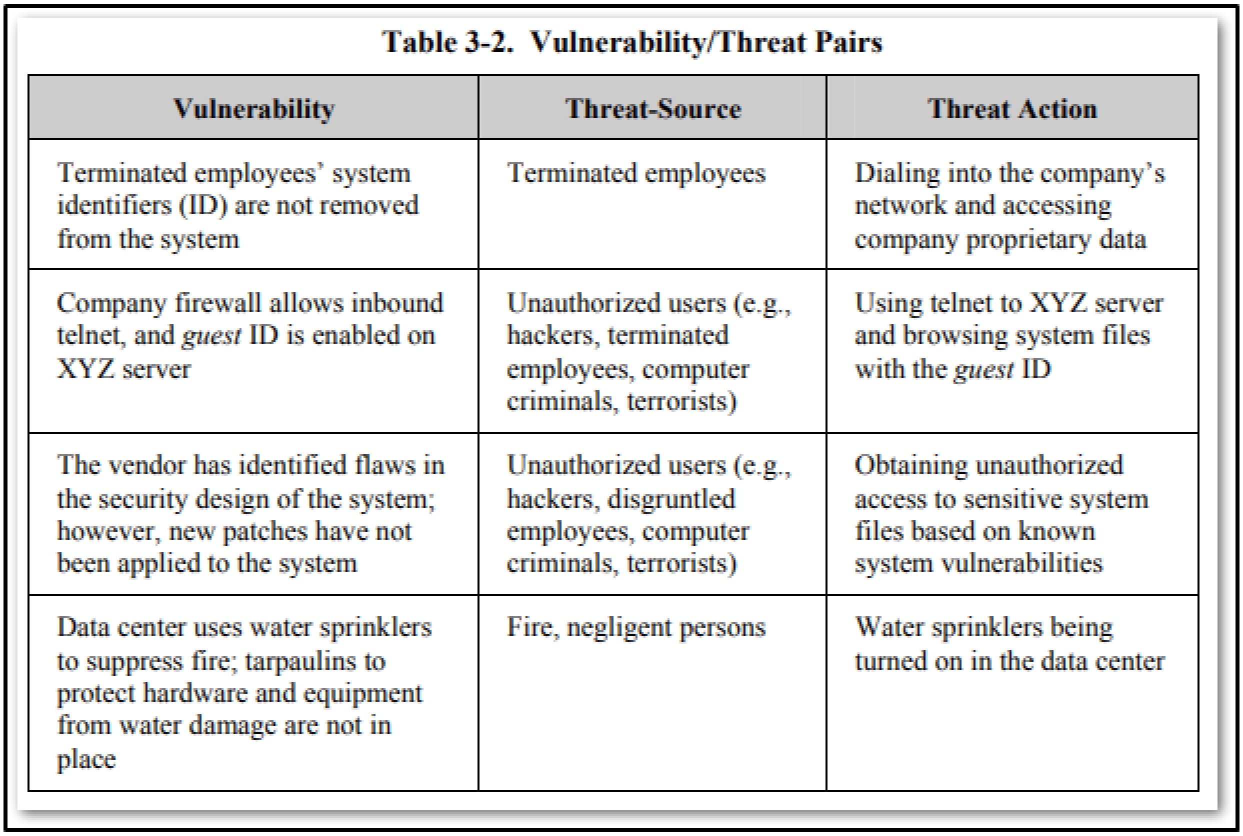


Table 3-2. Vulnerability/Threat Pairs

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Vulnerability Sources

- Previous risk assessment documentation of the IT system assessed
- The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
- Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- System software security analyses.

System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently. Test methods include:

- Automated vulnerability scanning tool
- Security test and evaluation (ST&E)
- Penetration testing

Development of Security Requirements Checklist

A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, information).

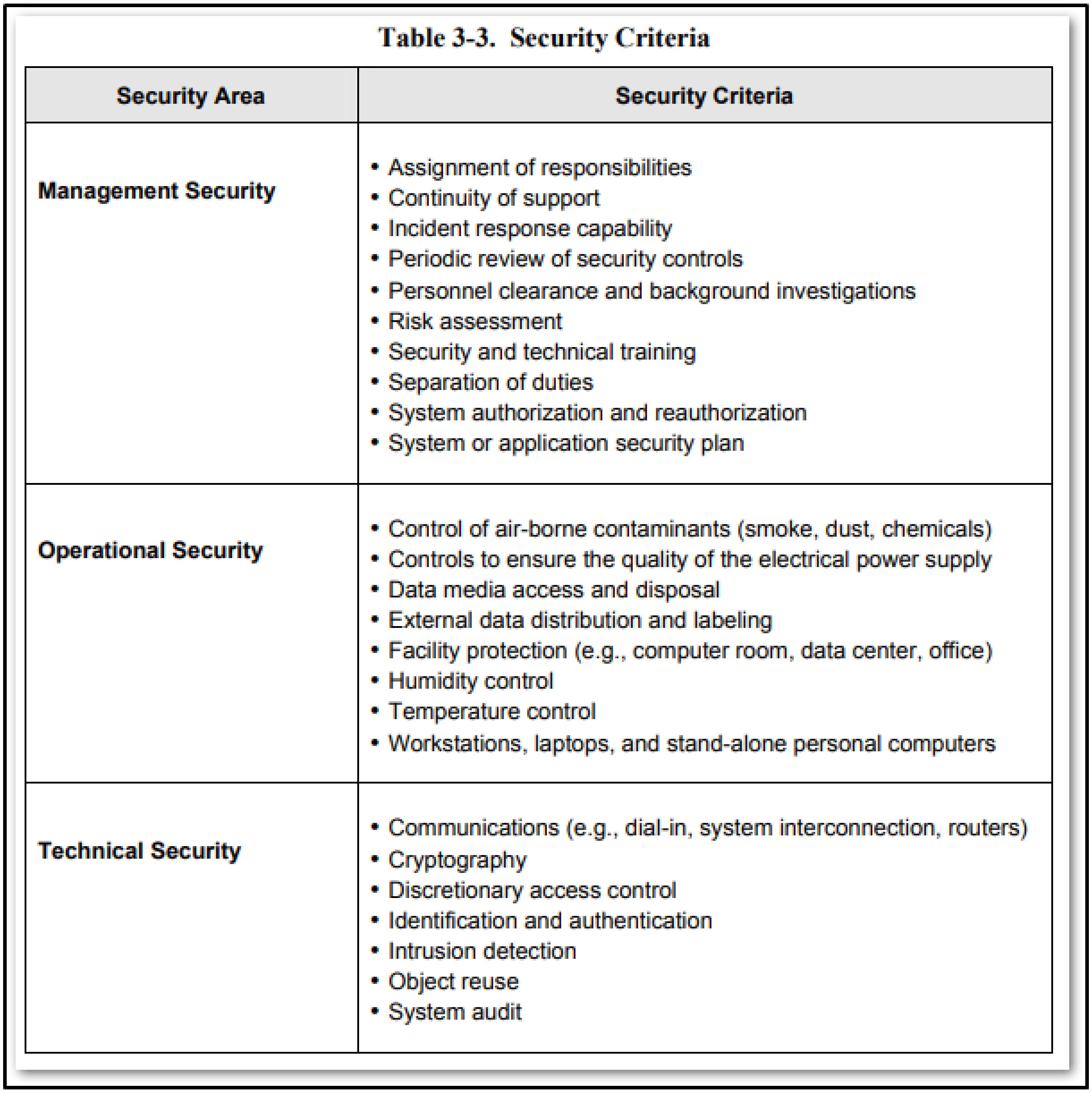


Table 3-3. Security Criteria

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • 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	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

The outcome of this process is the security requirements checklist.

The *NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems*, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Output from Step 3 - A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources

Step – 4: Control Analysis

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

Controls Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software. Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective.

Control Analysis Techniques

As discussed, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner.

Output from Step 4 - List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event

Step – 5: Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

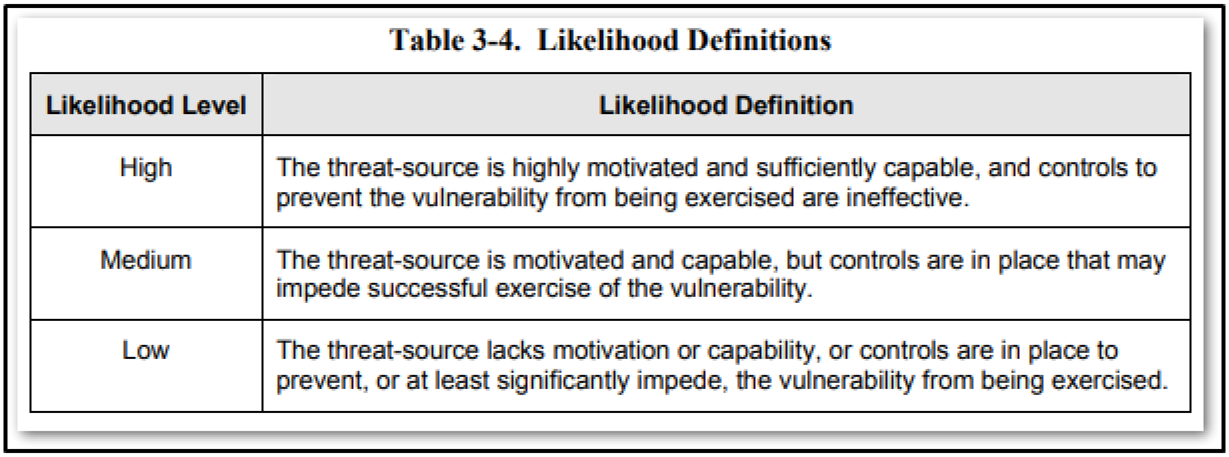


Table 3-4. Likelihood Definitions

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

Output from Step 5 - Likelihood rating (High, Medium, Low)

Step – 6: Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- System mission (e.g., the processes performed by the IT system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity.

This information can be obtained from existing organizational documentation, such as the mission impact analysis report (business impact analysis [BIA]) or asset criticality assessment report. If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information.

The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification.
- **Loss of Availability:** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected.
- **Loss of Confidentiality:** System and data confidentiality refers to the protection of information from unauthorized disclosure.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts.

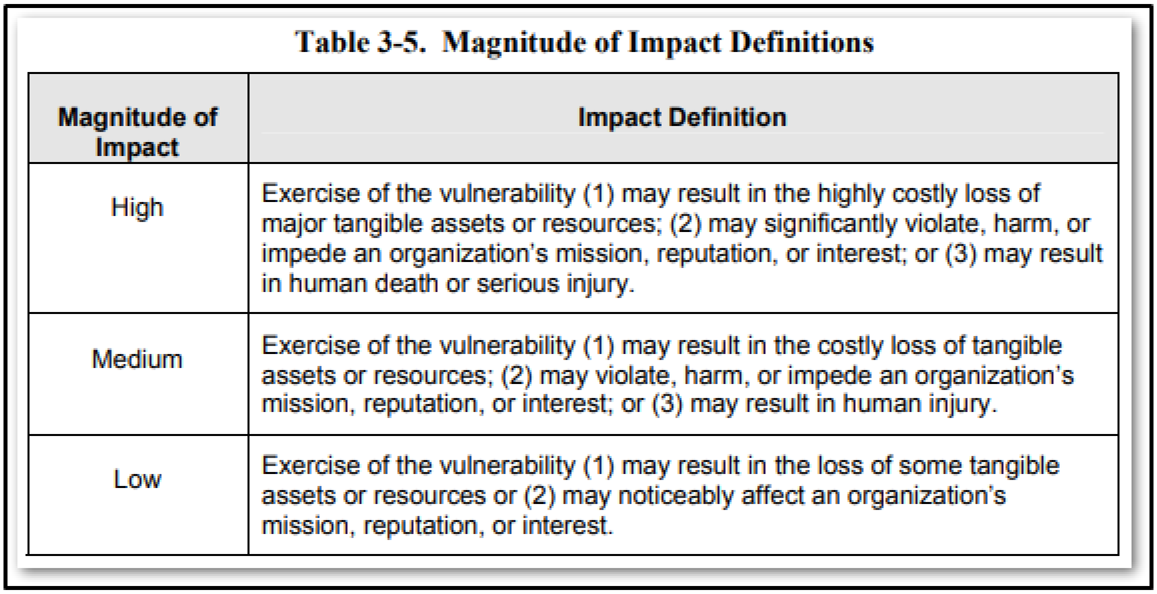


Table 3-5. Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Quantitative versus Qualitative Assessment

	Qualitative Assessment	Quantitative Assessment
Advantage	It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.	It provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis.
Disadvantage	It does not provide specific quantifiable measurements of the magnitude of the impacts to perform cost-benefit analysis.	The numerical ranges used to express the measurement results in unclear qualitative measurements.

Quantitative Risk Assessment Formula

Quantitative risk assessment takes a more rigorous approach, using numeric data to perform risk calculations in terms of financial value. This requires the use of several factors and formulas:

- Organizations must first identify the ***asset value (AV)*** for each asset covered by the risk assessment. AV is normally expressed in terms of dollar value. This can be done by using a variety of valuation techniques, such as purchase price, replacement cost, or depreciated value.
- For each risk facing an asset, the risk assessment process next identifies the ***exposure factor (EF)***. The exposure factor is the amount of damage that would occur to an asset if the risk was to materialize; this is normally expressed as a percentage. For example, if the risk of fire is likely to destroy half of a data center, the EF is 50 percent.
- The last input into the quantitative risk assessment process is ***the annualized rate of occurrence (ARO)***. This is the likelihood that the risk will materialize. It is expressed as the number of times the risk is expected to occur in a typical year. The value may be less than one if the risk is expected less than once per year.

- Next, the risk assessment process calculates the ***single loss expectancy (SLE).*** This is the impact of the risk, expressed as the financial loss that occurs each time the risk materializes; it is calculated by using this formula:
- ***SLE = AV × EF***
- Finally, the risk is calculated as the product of likelihood (ARO) and impact (SLE) by using this formula:
  ALE = SLE × ARO
  This formula provides the ***annualized loss expectancy (ALE),*** or the expected financial loss that will occur due to the risk in a typical year.

Let's work through an example of quantitative risk assessment.
Consider a data center located in the San Francisco Bay Area. Risk managers for the firm owning the data center would certainly be interested in assessing the risk associated with an earthquake damaging the data center. Here's the process they would go through to do this by using quantitative techniques:

1. Identify the asset value (AV). They might do this by consulting data center construction experts and determining that the replacement cost of the data center would be $20 million. (AV = $20 million)
2. Determine the exposure factor (EF). Consulting with those same experts might identify that the data center would be half destroyed by a significant earthquake. (EF = 50 percent)
3. Identify the annualized rate of occurrence (ARO). This is the likelihood of an earthquake occurring in a particular year. The US Geological Survey estimates that the Bay Area is likely to suffer an earthquake causing extensive damage once every 30 years. (ARO = 0.03)
4. Calculate the single loss expectancy (SLE). This is the impact of an earthquake, expressed as the financial loss that a single earthquake would create, and is calculated as the product of the asset value and exposure factor:
   SLE = AV × EF SLE => $20 million × 50 percent SLE = $10 million
5. Calculate the annualized loss expectancy (ALE). This is the risk, expressed as the financial loss from earthquakes expected in a typical year:
   ALE = SLE × ARO ALE = $10 million × 0.03 ALE = **$300,000**

A risk manager can now use the annualized loss expectancy to make risk-based decisions. For example, an earthquake insurance policy with a $50,000 annual premium would be a good investment!

Output from Step 6 - Magnitude of impact (High, Medium, or Low)

Step – 7: Risk Determination

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed.

Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact.

For example,

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

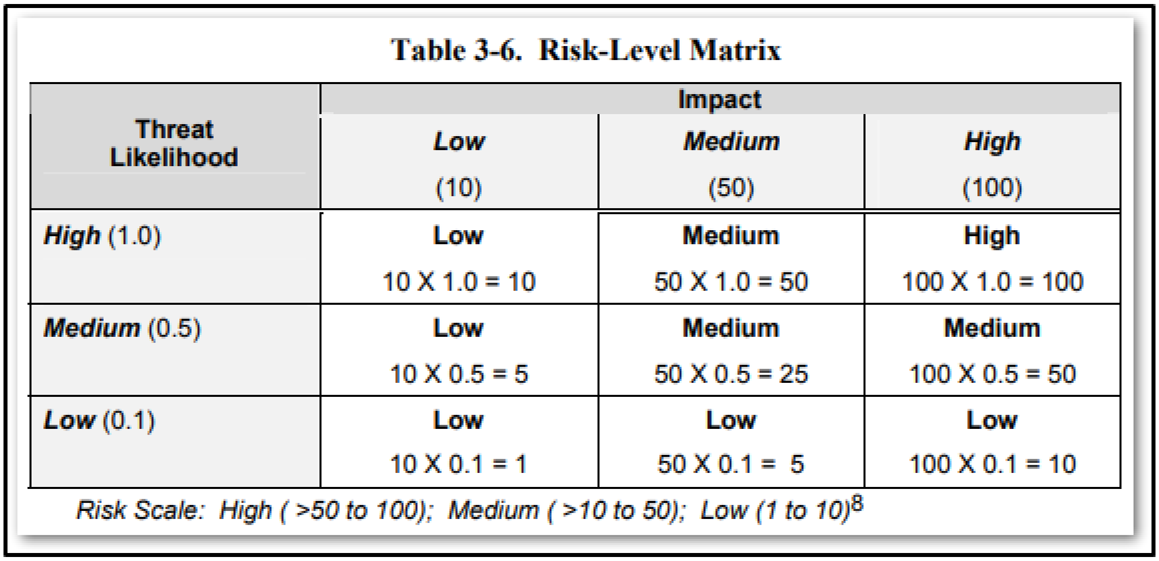


Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Description of Risk Level

Following table describes the risk levels shown in the above matrix. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

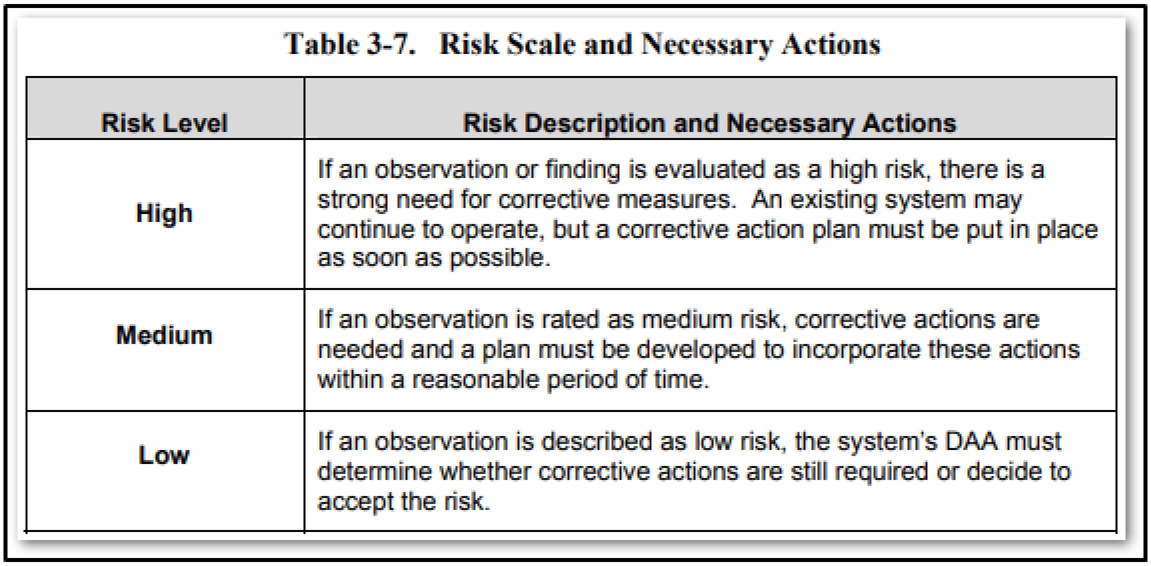


Table 3-7. Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	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.
Medium	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.
Low	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.

Output from Step 7 – Risk level (High, Medium, Low)

Step – 8: Control Recommendation

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

Output from Step 8 - Recommendation of control(s) and alternative solutions to mitigate risk

Step – 9: Result Documentation

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

Output from Step 9 - Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation

Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process.

Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the ***least-cost approach*** and implement the ***most appropriate controls*** to decrease mission risk to an acceptable level, with ***minimal adverse impact*** on the organization's resources and mission.

Risk Mitigation Options / Strategies

Risk mitigation can be achieved through any of the following risk mitigation options:

Risk Assumption / Acceptance: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

Risk Avoidance: To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)

Risk Limitation: To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

Risk Planning: To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls

Research and Acknowledgment: To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability

Risk Transference: To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.

Risk Mitigation Strategy

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organization?"

The risk mitigation chart in addresses these questions.

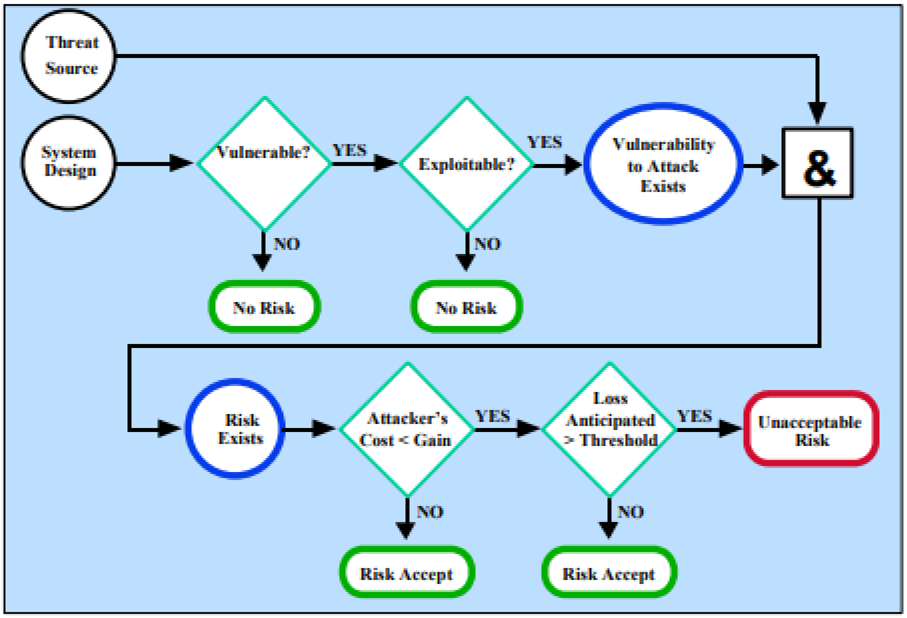


Figure 4-1. Risk Mitigation Action Points

In simple words, when the risk gets to the level of unacceptable the action must be initiated.

Approach for Control Implementation

When control actions must be taken, the following rule applies:

Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.

The following risk mitigation methodology describes the approach to control implementation:

Steps	Action	Output
Step – 1	**Prioritize Actions:** Based on the risk levels presented in the risk assessment report	*Actions ranking from High to Low*
Step – 2	**Evaluate Recommended Control Options:** Evaluate the controls recommended in the risk assessment process	*List of feasible controls*
Step – 3	**Conduct Cost-Benefit Analysis:** To aid management in decision making and to identify cost-effective controls, a cost-benefit analysis is conducted.	*Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls*
Step – 4	**Select Control:** On the basis of the results of the cost-benefit analysis, management determines the most cost-effective control(s)	*Selected control(s)*
Step – 5	**Assign Responsibility:** Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is	*List of responsible persons*

	assigned	
Step – 6	**Develop a Safeguard Implementation Plan:** During this step, a safeguard implementation plan (or action plan) is developed. The plan should, at a minimum, contain the following information: • Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report) • Recommended controls • Prioritized actions • Selected planned controls • Required resources for implementing the selected planned controls • Lists of responsible teams and staff • Start date for implementation • Target completion date for implementation • Maintenance requirements	*Safeguard implementation plan*
Step – 7	**Implement Selected Control(s):** Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk.	*Residual risk*

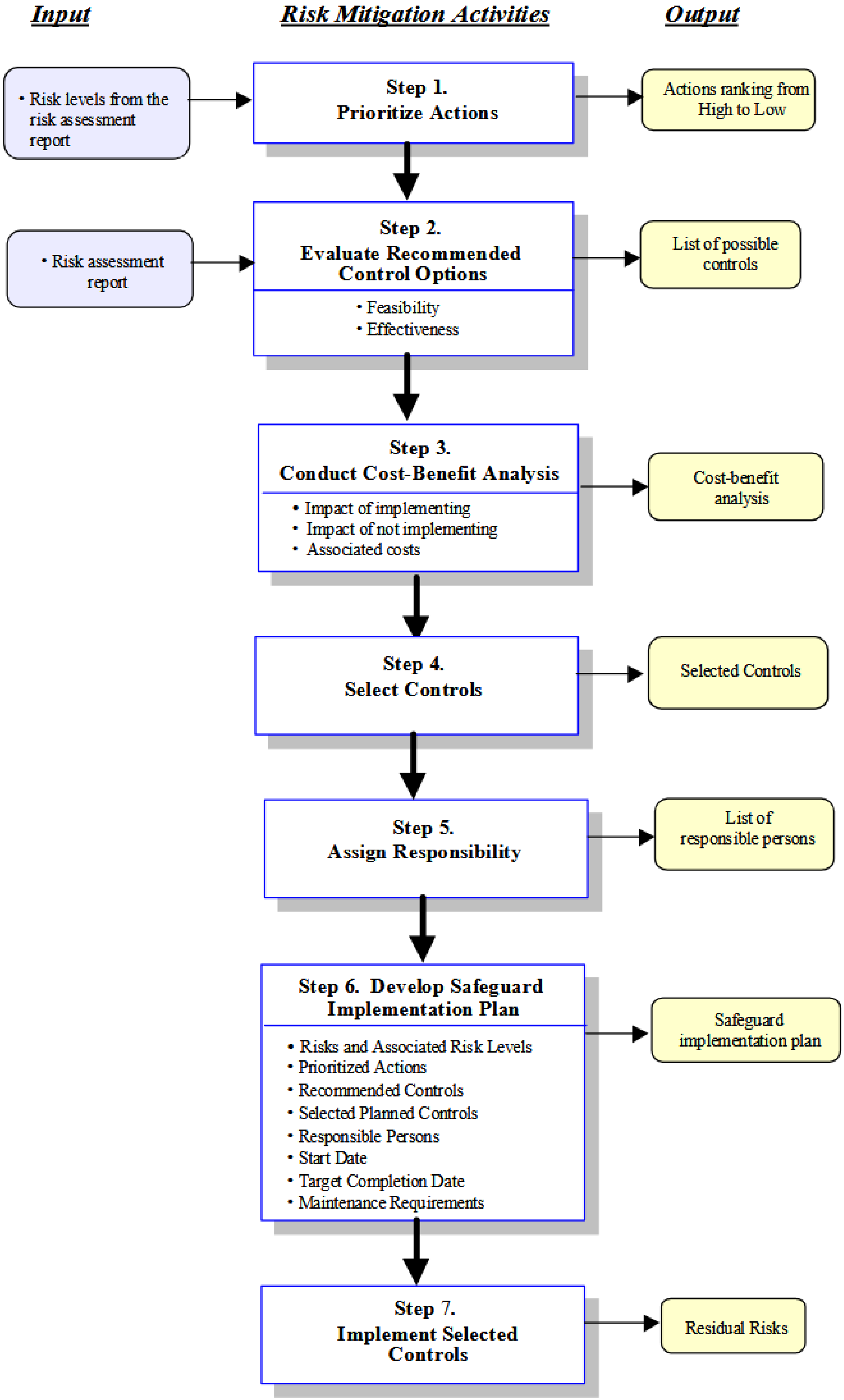
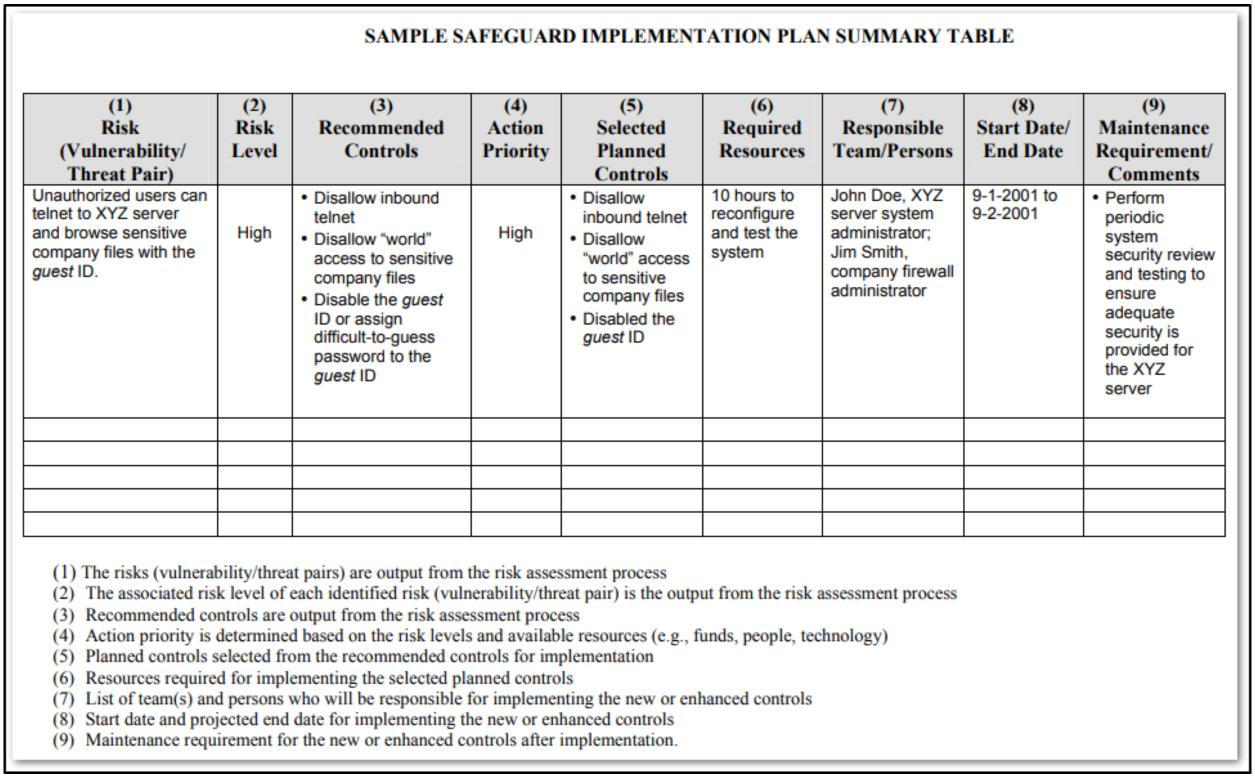

Input
Risk Mitigation Activities
Output
• Risk levels from the risk assessment report
Step 1.
Prioritize Actions
Actions ranking from High to Low
• Risk assessment report
Step 2.
Evaluate Recommended Control Options
• Feasibility
• Effectiveness
List of possible controls
Step 3.
Conduct Cost-Benefit Analysis
• Impact of implementing
• Impact of not implementing
• Associated costs
Cost-benefit analysis
Step 4.
Select Controls
Selected Controls
Step 5.
Assign Responsibility
List of responsible persons
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
Safeguard implementation plan
Step 7.
Implement Selected Controls
Residual Risks

Figure 4-2. Risk Mitigation Methodology Flowchart



SAMPLE SAFEGUARD IMPLEMENTATION PLAN SUMMARY TABLE

(1) Risk (Vulnerability/ Threat Pair)	(2) Risk Level	(3) Recommended Controls	(4) Action Priority	(5) Selected Planned Controls	(6) Required Resources	(7) Responsible Team/Persons	(8) Start Date/ End Date	(9) Maintenance Requirement/ Comments
Unauthorized users can telnet to XYZ server and browse sensitive company files with the *guest* ID.	High	• Disallow inbound telnet • Disallow "world" access to sensitive company files • Disable the *guest* ID or assign difficult-to-guess password to the *guest* ID	High	• Disallow inbound telnet • Disallow "world" access to sensitive company files • Disabled the *guest* ID	10 hours to reconfigure and test the system	John Doe, XYZ server system administrator; Jim Smith, company firewall administrator	9-1-2001 to 9-2-2001	• Perform periodic system security review and testing to ensure adequate security is provided for the XYZ server

(1) The risks (vulnerability/threat pairs) are output from the risk assessment process
(2) The associated risk level of each identified risk (vulnerability/threat pair) is the output from the risk assessment process
(3) Recommended controls are output from the risk assessment process
(4) Action priority is determined based on the risk levels and available resources (e.g., funds, people, technology)
(5) Planned controls selected from the recommended controls for implementation
(6) Resources required for implementing the selected planned controls
(7) List of team(s) and persons who will be responsible for implementing the new or enhanced controls
(8) Start date and projected end date for implementing the new or enhanced controls
(9) Maintenance requirement for the new or enhanced controls after implementation.

Control Categories

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an organization's mission.

Technical Security Controls

Technical security controls for risk mitigation can be configured to protect against given types of threats. Technical controls can be grouped into the following major categories, according to primary purpose:

- **Support:** Supporting controls are generic and underlie most IT security capabilities. These controls must be in place in order to implement other controls.
- **Prevent:** Preventive controls focus on preventing security breaches from occurring in the first place.
- **Detect and Recover:** These controls focus on detecting and recovering from a security breach.

Following figure depicts the primary technical controls and the relationships between them.

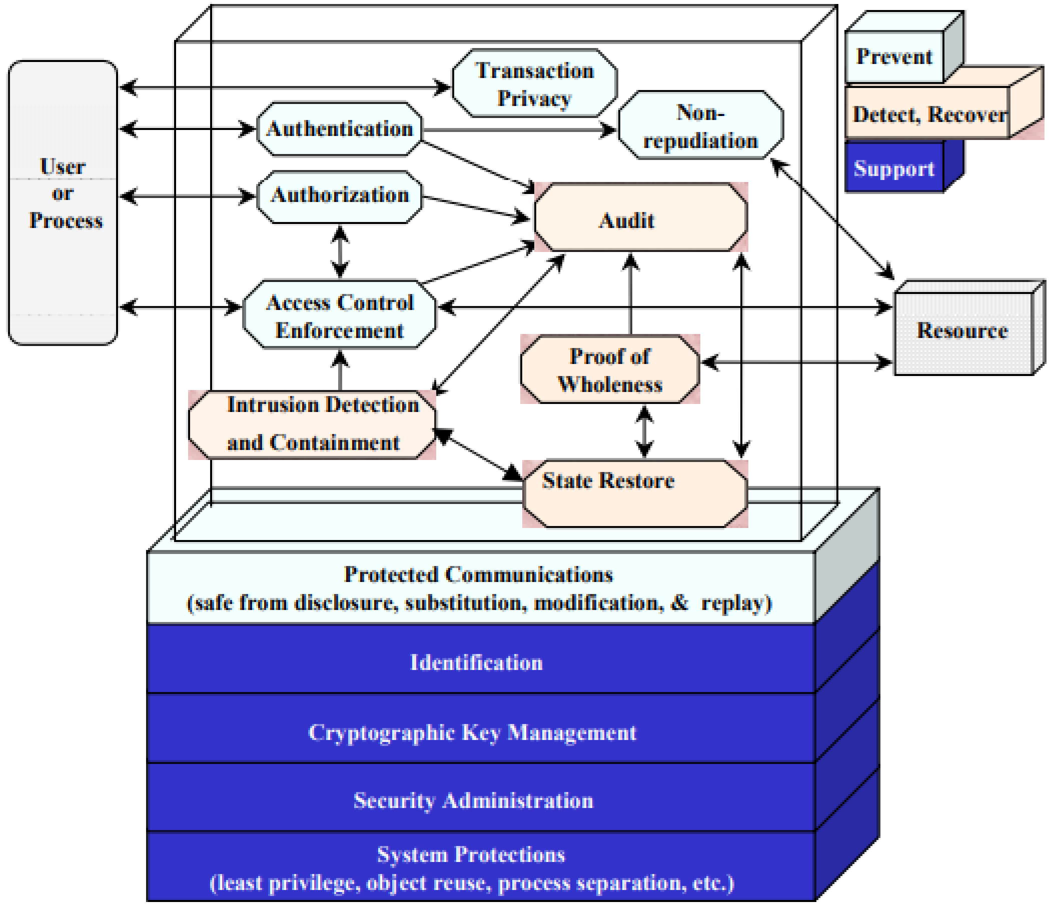


Figure 4-3. Technical Security Controls

Management Security Controls

Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management security control further divided into preventive, detection, and recovery controls.

Preventive Management Security Controls	• Assign security responsibility • Develop and maintain system security plans • Implement personnel security controls, including separation of duties, least privilege, and user computer access registration and termination • Conduct security awareness and technical training
Detection Management Security Controls	• Implement personnel security controls, including personnel clearance, background investigations, rotation of duties • Conduct periodic review of security controls • Perform periodic system audits • Conduct ongoing risk management to assess and mitigate risk • Authorize IT systems to address and accept residual risk.
Recovery Management Security Controls	• Provide continuity of support • Establish an incident response capability

Operational Security Controls

Operational controls, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exercised by potential threat-sources.

Preventive Operational Controls	• Control data media access and disposal • Limit external data distribution • Control software viruses • Safeguard computing facility (e.g., security guards, site procedures for visitors, electronic badge system, biometrics access control, management and distribution of locks and keys, barriers and fences) • Secure wiring closets • Provide backup capability • Establish off-site storage • Protect laptops, personal computers (PC), workstations • Protect IT assets from fire damage • Provide emergency power source (e.g., requirements for uninterruptible power supplies, on-site power generators) • Control the humidity and temperature of the computing facility (e.g., operation of air conditioners, heat dispersal)
Detection Management Security Controls	• Provide physical security (e.g., use of motion detectors, closed-circuit television monitoring, sensors and alarms) • Ensure environmental security (e.g., use of smoke and fire detectors, sensors and alarms).

Cost Benefit Analysis

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk.

A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:

- Determining the impact of implementing the new or enhanced controls
- Determining the impact of not implementing the new or enhanced controls
- Estimating the costs of the implementation
- Assessing the implementation costs and benefits against system and data criticality

Residual Risk

The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.

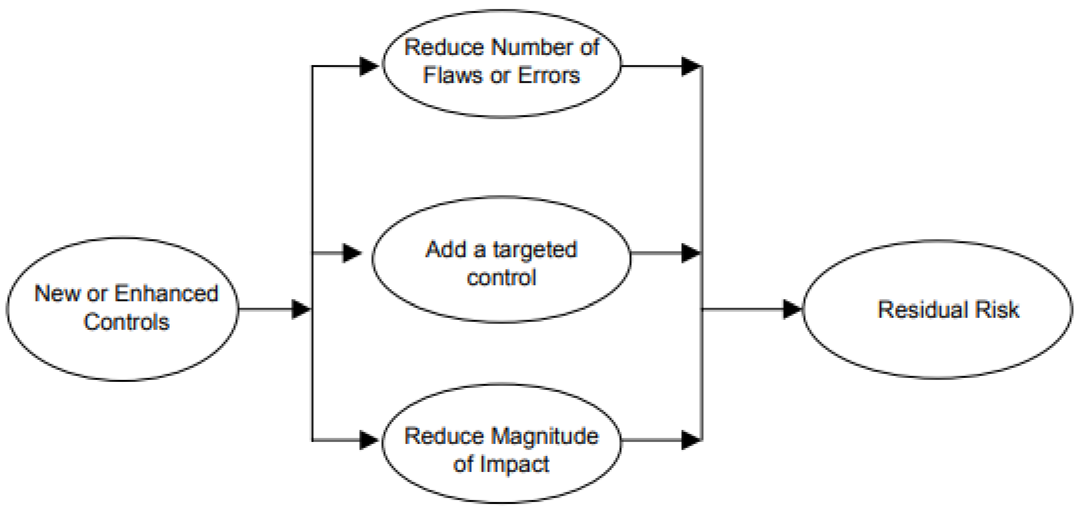


Figure 4-4. Implemented Controls and Residual Risk

Evaluation and Assessment

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

Good Security Practice

The risk assessment process is usually repeated at least every 3 years for federal agencies. However, risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization’s business objectives or mission

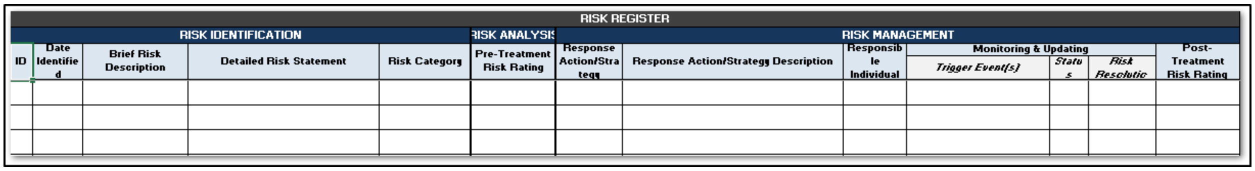
Keys for Success

A successful risk management program will rely on:

- Senior management’s commitment
- The full support and participation of the IT team
- The competence of the risk assessment team
- The awareness and cooperation of members of the user community
- An ongoing evaluation and assessment of the IT-related mission risks.

Risk Register

A risk register is a document used as a risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures. It can be displayed as a scatterplot or as a table.



RISK REGISTER												
RISK IDENTIFICATION					RISK ANALYSIS	RISK MANAGEMENT						
ID	Date Identified	Brief Risk Description	Detailed Risk Statement	Risk Category	Pre-Treatment Risk Rating	Response Action/Strategy	Response Action/Strategy Description	Responsible Individual	Monitoring & Updating			Post-Treatment Risk Rating
									Trigger Event(s)	*Status*	*Risk Resolutio*	

Practical Example

As we have learned that **Risk management** encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. In the following example we will perform a practical risk management process excluding *evaluation & assessment* phase which is the last phase and is mostly about monitoring and control assessment status.

Problem

Given a scenario perform risk management for a **XYZ** insurance firm that handles and process sensitive information and is subjected to privacy regulations in country.

Risk Assessment

Starting with risk assessment phase.

Step – 1: System Characterization

Organization Personnel main asset for organization as they process day to day **personally identifiable information** and business proprietary information

Step – 2: Threat Identification

Human threat is the main threat-source here for personnels.

Threat-Source	Motivation	Threat Actions
Hacker	Challenge Money Challenge Empower	Social Engineering Unauthorized Access Malware Infection Information Theft
Industrial espionage	Competitive advantage	Information theft Social Engineering

Step – 3: Vulnerability Identification

Personnel are vulnerable to social engineering and phishing attacks

Vulnerability	Threat-Source	Threat Action
People are not cyber aware	Hacker, espionage	Threat-sources could run a social engineering / phishing campaign in order to obtain sensitive proprietary company information or unauthorized access to organization systems.

Step – 4: Control Analysis

Vulnerability	Threat-Source	Threat Action	Current / Planned Controls
People are not cyber aware	Hacker, espionage	Threat-sources could run a social engineering / phishing campaign in order to obtain sensitive proprietary company information or unauthorized access to organization systems.	There is spam filter in place that filters emails and sends unsolicited emails to spam. All endpoint have Anti-malware software installed.

Step – 5: Likelihood Determination

Likelihood of this threat is **high** as hackers and competitive groups are highly motivated to run this type of campaigns and it does not require expert skill level. A well-known hacker could take advantage of existing tools to run this campaign.

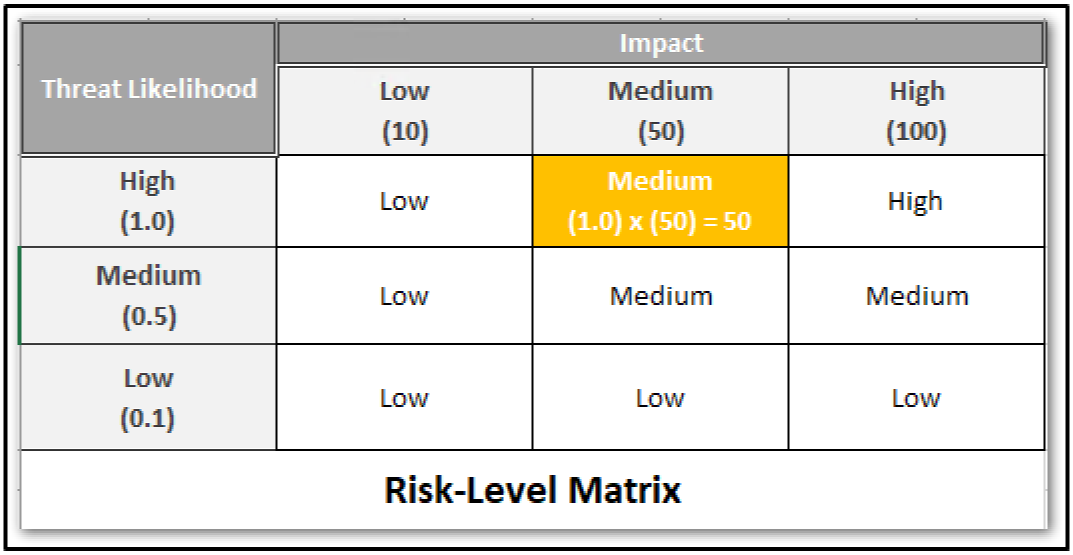
Step – 6: Impact Analysis

Depending on the target personnel responsibilities the successful attack could result in information theft of any classification or in severe case the threat-source (attacker, threat-actor) could install malware to systems to obtain persistence access.

According to above statement the overall impact of this attack is **medium**.

This is qualitative analysis but quantitative assessment should be performed as well.

Step – 7: Risk Determination



Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low	Medium (1.0) x (50) = 50	High
Medium (0.5)	Low	Medium	Medium
Low (0.1)	Low	Low	Low

Risk-Level Matrix

Step – 8: Control Recommendation

Vulnerability	Threat-Source	Threat Action	Current / Planned Controls	Recommended Controls
People are not cyber aware	Hacker, espionage	Threat-sources could run a social engineering / phishing campaign in order to obtain sensitive proprietary company information or unauthorized access to organization systems.	There is spam filter in place that filters emails and sends unsolicited emails to spam. All endpoint have Anti-malware software installed.	**1 -** It is highly recommended that there should be an effective cyber-security awareness program that should address phishing, social engineering and other human attacks and vulnerabilities **2 -** Implement a phishing prevention technology that should prevent phishing attacks.

Step – 9: Results Documentation

Above table should be documented as it is or in a report format.

Risk Mitigation

Risk Mitigation Options

This risk cannot be accepted and so the best mitigation option for this risk is **Risk Limitation** by applying recommended controls.

Control Implementation

In this phase further analysis on risk is performed and certain decisions are finalized. The most important part of this phase is **Implementation Plan Table**.

Risk (Vulnerability / Threat Pair)	Risk Level	Recommended Controls	Action Priority	Selected Controls	Responsible Team/ Persons	Start Date/ End Date	Maintenance / Comments
Hackers can run social engineering campaign to obtain sensitive information or unauthorized acces	Medium	**1 -** It is highly recommended that there should be an effective cybersecurity awareness program that should address phishing, social engineering and other human attacks and vulnerabilities. **2 -** Implement a phishing prevention technology that should prevent phishing attacks.	High	Create cyber-security awareness program and educate employees	Information Security Team	02-02-2020 To 02-05-2020	Create a training plain and inform board on progress on every second week.

Resources

https://www.smartsheet.com/free-risk-management-plan-templates