

Risk Management Plan

Risk management refers to the process of handling potential risks that an organization may encounter. This process involves the identification, evaluation, and mitigation of various threats that could compromise the confidentiality, integrity, and availability of an organization's assets. This document outlines various methodologies for identifying and evaluating these risks.

1. Risk Assessment Approach

Risk assessment is the process of identifying potential risks that could impact an organization's business operations. To ensure the security of its resources and business continuity, an organization should conduct risk assessments at regular intervals. This involves determining the risks the organization faces. To this end, organizations should employ security experts and establish a comprehensive plan for the process. The security personnel are required to meticulously document all actions taken to identify and evaluate the potential risks.

In this risks management plan, the security personnel must detail how they identified, the techniques they have used to identify, and so on. The following matrix can be used to simplify this task and systematically document their findings:

1.1 Participants Involved

The risk assessment process involves the following participants:

Role	Participants	Contact Details
System Owner		Phone: Email:
System Custodian		Phone: Email:
Security Administrator		Phone: Email:
Database Administrator		Phone: Email:

1.2 Techniques Used

Technique	Description	Status
[List techniques used, e.g., questionnaires, tools]	[Describe the technique used and how it assisted in performing the risk assessment]	

1.3 Risk Model

[Describe the risk model used in performing the risk assessment; refer to NIST publication SP-800-30 for an example risk model]

2. System Characterization

2.1 Technology Components

Component	Description	Status
Applications	[Describe key technology components, including commercial software]	
Databases		
Operating Systems		
Networks		
Interconnections		
Protocols		
Others (If any)		

2.2 Physical Location(s)

Location	Description
[Include locations included in scope]	

2.3 Data Used by System

Data	Description
[Detail data elements included in scope]	[Describe characteristics of data elements]

2.4 Users

Users	Description
[Detail categories of users]	[Describe how users access the system and their intended use of the system]

3. Threat and Vulnerability Identification

3.1 Vulnerability Statement

[Compile and list potential vulnerabilities applicable to the system assessed]

Vulnerability	Description
[List vulnerabilities]	[Describe vulnerability and its impact]

3.2 Threat Statement

[Compile and list the potential threat-sources applicable to the system assessed]

Threat-Source	Threat-Actions
[List threat sources]	[List and/or describe actions that can be taken by threat source, e.g., identity theft, spoofing, system intrusion]

List Risks	Identification Methods	Risk Category	Control Adequacy	Risk Status

The different methods to identify the potential risks:

- Program monitoring data
- Insurance claims history
- Audit and monitoring reports
- Accident reports
- Employee focus groups

The following are different risk categories:

- Employment practices
- Financial management practices
- Personal injury
- Property damage

Anticipating Vulnerability

The security personnel must document the assumptions that they have made about their organization's vulnerability to risks. The "risk matrix" table shown above is useful in assessing both the likelihood of occurrence and the severity of the consequences of risks.

Such assumptions can be assessed by simply inserting the "vulnerability to risk" worksheet in the plan using the following table.

- The security personnel must list out all the risks in this table as they have identified and listed in the previous table.
- They must figure out the factors that they considered could lead to the likelihood of the risk occurring.
- They must figure out the factors that they considered could lead to the severity of the risk occurring.
- They must assess the cost it takes to eradicate these risks or reduce their consequences.

Risks	Likelihood	Severity	Cost

Relative Vulnerability

Referring to the “vulnerability to risk” table above, the identified risks can be organized into the matrix table provided below. This arrangement facilitates a clearer understanding and assists in drawing conclusions about the relative urgency required to respond to these risks.

Green	Low
Yellow	Moderate
Orange	High
Red	Extreme

	Negligible	Marginal	Critical	Catastrophic
Certain				
Likely				
Passible				
Unlikely				
Rare				

Response to Risks

In this section, various mitigation strategies must be implemented to minimize the organization's exposure to risks. The table below outlines the strategies deployed and the security personnel responsible for their implementation. They are required to list the risks previously identified and noted in the prior tables.

Risk	Mitigation Strategies	Implementation Responsibility

Risk Mitigation Tracking Worksheet

Mitigation strategy being monitored: _____

Documents monitored (✓) _____ Application documents _____ Client files _____

Location: _____

Indicator Code Key

The security personnel must replace the numbers in the top row with the warning signs for risk mitigation strategy that they are tracking.

Key	1	2	3	4	5
1					
2					
3					
4					
5					

Mitigation Exceptions Identified

What has been monitored? _____ Sample size _____

Identifier	1	2	3	4	5	6	7	8	9	10

Monitor: _____ Position: _____ Date: _____

Signature: _____ Received by: _____ Date: _____

Corrective Action

When your tracking data shows a pattern of ineffectiveness, you need to develop a corrective action plan to restore your strategy's effectiveness. In this section, the security personnel must develop a corrective action plan to restore their strategies in case of failure of their tracking data.

A corrective action plan is a more narrowly focused version of a mitigation-tracking process. It has the same basic components, as outlined below.

Risk Management Corrective Action Plan

CAA Name: _____ Fiscal Year: _____

Risk _____ Strategy _____

Responsible _____ Date: _____

Causes identified in analysis	
Causes to be corrected	

List of Strategies	Specific Success Indicators to be Tracked	Mechanisms for Reporting Results to Top Management and the Board	Review the Strategies
1.	a.		
	b.		
	c.		
2.	a.		
	b.		
	c.		
3.	a.		
	b.		
	c.		