**Name of Organization**

**Risk Management Plan**

December 2021

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Risk Management Plan document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction 5](#_Toc90540556)

[Purpose Of The Risk Management Plan 5](#_Toc90540557)

[II. Risk Management Procedure 5](#_Toc90540558)

[Process 5](#_Toc90540559)

[Roles and Responsibilities 5](#_Toc90540560)

[Risk Identification 6](#_Toc90540561)

[Methods for Risk Identification 6](#_Toc90540562)

[Risk Analysis 6](#_Toc90540563)

[Qualitative Risk Analysis 7](#_Toc90540564)

[Quantitative Risk Analysis 7](#_Toc90540565)

[Risk Response Planning 7](#_Toc90540566)

[Risk Monitoring, Controlling, And Reporting 8](#_Toc90540567)

[Risk Contingency Budgeting 9](#_Toc90540568)

[III. Tools and Practices 9](#_Toc90540569)

[IV. Closing a Risk 9](#_Toc90540570)

[V. Lessons Learned 10](#_Toc90540571)

# Introduction

##

## Purpose Of The Risk Management Plan

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project’s objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, controlling, and reporting risks. This Risk Management Plan defines how risks associated with the <Project Name> project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks by the Risk Manager and/or Risk Management Team.

Risks related to IT systems or applications must be identified and documented based on the methodology in NIST SP 800-30, Risk Management Guide for Information Technology Systems. IT system or application weaknesses must be identified on an associated plan of action and milestones (POA&M) and tracked in accordance with NIST POA&M guidelines. Appropriate protective measures must be taken to safeguard sensitive IT system or application weaknesses or vulnerabilities from unauthorized disclosure.

# Risk Management Procedure

## Process

[Summarize the steps necessary for responding to project risk.]

The project manager working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the lifecycle of the project. Risks will be identified as early as possible in the project to minimize their impact. The steps for accomplishing this are outlined in the following sections of this document. The <project manager or other designee> will serve as the Risk Manager for this project.

A distinction may need to be made between overall project risk management and IT system or application risk management. Risks related to IT systems or applications must be identified and documented based on the methodology in NIST SP 800-30, Risk Management Guide for Information Technology Systems.

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| Business SME (BSME) | The BSME assists in identifying and determining the context, consequence, impact, timing, and priority of the risk.  |
| Risk Manager or Project Manager (PM) | The Risk Manager or PM is a member of the Integrated Project Team (IPT). The Risk Manager or PM determines if the Risk is unique, identifies risk interdependencies across projects, verifies if risk is internal or external to project, assigns risk classification and tracking number. During the life of the project, they continually monitor the project for potential risks. |
| Integrated Project Team (IPT) | The IPT is responsible for identifying the risks, the dependencies of the risk within the project, the context and consequence of the risk. They are also responsible for determining the impact, timing, and priority of the risk as well as formulating the risk statements. |
| Risk Owner(s) | The risk owner determines which risks require mitigation and contingency plans, he/she generates the risk mitigation and contingency strategies and performs a cost benefit analysis of the proposed strategies. The risk owner is responsible for monitoring and controlling and updating the status of the risk throughout the project lifecycle. The risk owner can be a member of the project team.  |
| Other Key Stakeholders | The other stakeholders assist in identifying and determining the context, consequence, impact, timing, and priority of the risk.  |

## Risk Identification

Risk identification involves the project team, appropriate stakeholders, and includes an evaluation of environmental factors, organizational culture and the project management plan including the project scope, schedule, cost, or quality. Careful attention should be given to the project deliverables, assumptions, constraints, WBS, cost/effort estimates, resource plan, and other key project documents.

## Methods for Risk Identification

The following methods are used to assist in the identification of risks associated with <Project Name>:

* Brainstorming
* Interviewing
* SWOT (Strengths, Weaknesses, Opportunities and Threats)
* Diagramming
* Etc.

A Risk Management Log should be generated and updated as needed and should be stored electronically in the project library located at <file location>.

## Risk Analysis

All risks identified should be assessed to identify the range of possible project outcomes. Risks are prioritized by their level of importance.

##

## Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk should be assessed by the project manager, with input from the project team using the following approach:

**Probability**

* High – Greater than <70%> probability of occurrence
* Medium – Between <30%> and <70%> probability of occurrence
* Low – Below <30%> probability of occurrence

**Impact**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Impact | H |  |  |  |
| M |  |  |  |
| L |  |  |  |
|  | L | M | H |
|  | Probability |

* High – Risk that has the potential to greatly impact project cost, project schedule or performance
* Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
* Low – Risk that has relatively little impact on cost, schedule, or performance

Risks that fall within the RED and YELLOW zones will have a risk response plan which should include both a risk response strategy and a risk contingency plan.

##

## Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities should be estimated, a numerical rating is applied to each risk based on quantitative analysis, and then documented in this section of the risk management plan.

##

## Risk Response Planning

Each major risk (those falling in the Red & Yellow zones) should be assigned to a risk owner for monitoring and controlling purposes to ensure that the risk will not “fall through the cracks”.

For each major risk, one of the following approaches are selected to address it:

* **Remediate** – fix the underlying threat or condition
* **Avoid** – Eliminate the threat or condition or to protect the project objectives from its impact by eliminating the cause
* **Mitigate** – Identify ways to reduce the probability or the impact of the risk
* **Accept** – Nothing will be done
* **Contingency** –Define actions to be taken in response to risks
* **Transfer** – Shift the consequence of a risk to a third party together with ownership of the response by making another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk to be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc. Any secondary risks that result from risk mitigation response will be documented and follow the risk management protocol as the primary risks.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined if the risk does materialize to minimize its impact.

##

## Risk Monitoring, Controlling, And Reporting

The level of risk on a project will be tracked, monitored, controlled and reported throughout the project lifecycle. [Describe the methods and metrics that will be used to track the project’s risk status throughout the lifecycle as well as how this status will be reported to the stakeholders/ management.]

Risks should be assigned a risk owner(s) who will track, monitor, control and report on the status and effectiveness of each risk response action to the Project Manager and Risk Management Team on a <insert timeframe>.

A “Top 10 Risk List” should be maintained by the PM/Risk Manager or IPT and will be reported as a component of the project status reporting process for this project.

All project change requests will be analyzed for their possible impact to the project risks.

As Risk Events occur, the list will be re-prioritized during weekly reviews and risk management plan will reflect all changes to the risk lists including secondary and residual risks.

Management will be notified of important changes to risk status as a component to the Executive Project Status Report. [State timeframe, i.e., every two weeks]

The Risk Manager (PM) will:

* Review, reevaluate, and modify the probability and impact for each risk item [timeframe, as needed, every two weeks, etc.]
* Analyze any new risks that are identified and add these items to the risk list (or risk database).
* Monitor and control risks that have been identified
* Review and update the Top Ten risk list [timeframe, as needed, every two weeks, etc.]
* Escalate issues/ problems to management [List factors that would need to be escalated to management. Examples: documented mitigation actions are not effective or producing the desired results; the overall level of risk is rising.]

The Risk Owner will:

* Help develop the risk response and risk trigger and carry out the execution of the risk response if a risk event occurs.
* Participate in the review, re-evaluation, and modification of the probability and impact for each risk item on a weekly basis.
* Identify and participate in the analysis of any new risks that occur.
* Escalate issues/problems to PM that,
	+ Significantly impact the projects triple constraint or trigger another risk event to occur.
	+ Require action prior to the next weekly review
	+ Risk strategy is not effective or productive causing the need to execute the contingency plan.

Risk activities will be recorded in the <Document Name/ Risk Database Name> located on <full network path location>.

## Risk Contingency Budgeting

A risk contingency budget can be established to prepare in advance for the possibility that some risks will not be managed successfully. The risk contingency budget should contain funds that can be used so that your project doesn't go over budget.

There is a total of <$X> in the <Project Name> Project budget allocated for Risk Management activities. These activities may include, but are not limited to, identifying, analyzing, tracking, controlling, managing, and planning for risks. This also includes creating and updating the risk response strategies and contingency plans.

[Above is only an example of text that could be used. Enter whatever information is appropriate to outline/ define the budget associated with the Risk Management activities on the project.]

# Tools and Practices

A Risk Management Log will be maintained by the project manager and will be reviewed as a standing agenda item for project team meetings.

Risk activities will be recorded in the <Document Name/ Risk Database Name> located on <full network path location>.

# Closing a Risk

A risk will be considered closed when it meets the following criteria:

* <List the criteria when a risk can be closed>
* <Who has the authority to close a risk? >

Examples:

* Risk is no longer valid
* Risk Event has occurred
* Risk is no longer considered a risk

#  Lessons Learned

The lessons learned will be captured and recorded in the <Document Name/ Risk Database Name/Lessons Learned document or folder> located on <full network path location>.