



CARTER SUPPLY

Policies and Procedures

February 2, 2022

Risk Management Plan

Version 1.0

POLICIES AND PROCEDURES

Risk Management Plan

Prepared For

Carter Supply
Cityplace Center East
1212 North Main Avenue
Dallas, Texas 75204

Prepared By

Steve E. Nicholson, PMP

Table of Contents

Revision History	2
Introduction	3
Purpose of the Risk Management Plan.....	3
Background Information	3
Risk Approach	3
Approvals	4
Risk Management Processes	5
Risk Overview	5
Risk Identification	5
Risk Quantification	6
Risk Response Development.....	6
Risk Response Control.....	7
Risk Tools.....	7
Appendix A – Risk Form	8
Usage	8
Field Descriptions.....	8
Appendix B – Risk Report	10
Usage	10
Field Descriptions.....	10

Revision History

Date	Author	Version	Description
02/02/22	Steve E. Nicholson	1.0	Document created.

Introduction

Purpose of the Risk Management Plan

The purpose of this plan is to document the risk management practices and processes that will be used on programs and projects within Information Systems (IS).

Background Information

Risk is inevitable. There are risks on every project. But the impact of risks to a project can be diminished through preparation and planning. The “Risk Management Plan” will be the communication tool used by the project teams in planning for risk. At the minimum, the execution of the plan will make visible risks and their impacts to the project so no one is surprised should the risks occur. The optimum case, of course, is that, through the execution of the plan, the negative impact of the risk to the project is reduced or eliminated.

Risk Approach

The approach to risk for IS will be based on communication. All team members should actively be thinking of risks to the project. As risks are discovered, the processes and tools described in this management plan should be used to record and communicate the risks to the rest of the team. These processes will also quantify the impact of the risks and provide tools for recording mitigation or avoidance plans.

The program or project manager will act as risk manager. The responsibilities of the risk manager are:

- Solicit team members for new risks.
- Ensure new risks are recorded in the risk database.
- Track impact information from the appropriate team members.
- Work with team members to determine the best ways of addressing identified risks.
- After triggers are determined for a risk, work with the team members on a scheduled basis to determine if a trigger has occurred.

Risk Management Processes

Risk Overview

Risk management is concerned with maximizing positive events, or opportunities, and reducing the impact of negative events to the project. The definition of a risk is an event that has a probability of happening; an event that is already occurring, or is a certainty, is an issue and should be treated as such.

There are four main processes involved in risk management: risk identification, risk quantification, risk response development and risk response control.

These processes do not just occur at the start of the project; they occur throughout the entire project life cycle.

Risk identification involves determining which risks are likely to affect the project and documenting the characteristics of each.

Risk quantification is evaluating risks and risk interactions to assess the impact of the risks to the project.

Risk response development concerns responses to risks with negative impacts, or steps to take to increase positive opportunities.

Risk response control involves the evolution of risk responses as risk characteristics change during the life of the project.

The information on risk in this section comes from the Project Management Body of Knowledge (PMBOK) 2000 published by the Project Management Institute.

Risk Identification

Risk identification is the responsibility of every stakeholder on the project. Risks can be identified at any point in time. In order to keep risk identification in the minds of the team members, risk identification will be part of the project management risk, issue and change management meetings.

During these meetings, each participant will be asked for any new risks that might have surfaced since the previous meeting. Each risk that is identified will be recorded in the action item list by the risk manager. The participant will be asked to log the risk in the risk database. The characteristics of the risk will be recorded. These include values such as risk name, risk statement, consequence/opportunity, risk owner (assigned to), risk source, impact, probability of occurrence, exposure, risk response strategy, contingency plan, trigger and revised exposure. **Until risk quantification is performed, only risk name, statement, risk owner and consequence/opportunity should be recorded.**

The Risk Report will contain summary information for risks. The Risk Form will contain the details.

Risk Quantification

Risk quantification is primarily concerned with determining which risk events, according to their exposure factor, warrant a response.

The primary method we will use to quantify the risk exposure is by using values for probability and impact. The probability that a risk event will occur is high (1.0), medium (0.5) or low (0.1). The impact of the risk event is high (10), medium (5) or low (1). Probability is usually based on expert opinion. Impact is based on criteria established by the program manager to determine values for high, medium or low. For example, a schedule deviation of 1 month may be considered high, 1 week medium, and 1 day low.

To determine the risk exposure, the numerical equivalent of the probability is multiplied by the numerical equivalent of the impact.

Once all of the risk events are recorded, the risk exposure for each event should be calculated. The list is then sorted, with the risks with the highest exposure at the top. The risk exposure threshold will be 1 (possible risk exposure values are 10, 5, 2.5, 1, .5, .1). Only the risks that are above the exposure threshold should be analyzed further for the rest of the risk characteristics in the Risk Response Development phase.

The risk manager will work with the appropriate risk owner to determine the exposure.

Risk Response Development

Risk response development involves the defining of steps for addressing risks with risk impact values above the risk exposure threshold. For opportunities, these steps are enhancing the values. For threats, the steps are responses to the threat.

There are three general categories for responses to threats:

1. Avoidance - eliminating the cause of a risk may eliminate the risk itself. All risks cannot be avoided, but sometimes specific risks can.
2. Mitigation - reducing the exposure to a risk event, either by decreasing the probability of occurrence, the impact, or both.
3. Acceptance - accepting the consequences of the risk. If the risk cannot be avoided or mitigated, acceptance is the remaining category. Acceptance can be active, such as developing a contingency plan to execute, or passive, such as accepting a lower profit if the risk event occurs.

For the risk threats whose exposure value exceeds the defined threshold, the risk manager will work with the risk owner to select the response category and any response plan. For opportunities, the risk manager and risk owner will develop appropriate steps to enhance the project to work towards that opportunity.

Risk Response Control

Risk response control involves the execution of the risk management plan to respond to risks. It also involves executing the risk cycle of identification, quantification and response development when changes occur to the project. As the project progresses, the risk must be re-evaluated as changes will take place that may affect identified risks, or introduce new ones.

On a weekly basis, the risk manager will ask for feedback on previously identified risks or, if changes have occurred, or new information comes to light, ask for new risks to be identified.

Risk Tools

The risk tools that will be used are the Risk Management Plan (this document), the Risk Form and the Risk Report. The Risk Form will be a form in a database. The Risk Report will be a report in the same database.

To record a risk, a project team member should enter the information in a new record of the Risk Form located in the "RiskIssuesChanges" database in the ERP shared folder.

The above database for entering risks is located on the network under the share <<link provided here>>

Any updates to a risk can be done in the same form.

Please see the appendices for more detailed descriptions of the Risk Form and the Risk Report.

Appendix A – Risk Form

Usage

The Risk Form is used to enter new risks and maintain identified ones.

Detailed information about the risk will be maintained in this form. Summary information will be displayed in the Risk Report.

Field Descriptions

The Risk Identification Section is the first area to be completed for all new risks.

Ref

Reference number is an automatically generated numeric field.

Entry Date

The date the risk record was created.

Title

Title of the risk used as a short reference.

Description of Risk

A description of the risk. Also referred to as the risk statement.

Consequences

The ramifications, in narrative form, if the risk should occur.

Submitter

Name of the person submitting the risk.

Project Name

Name of the project with which the risk is associated.

Probability Factor

Probability of the risk occurring. 0.1 is low, 0.5 is medium, 1.0 is high.

Impact Factor

Impact of the risk to the project. 1 is low, 5 is medium, 10 is high.

Exposure

The result of the probability factor multiplied by the impact factor. Value of less than 1 is low/be aware, 1.0 – 2.5 is monitor carefully / outline plans, 5.0 – 10 is monitor closely / complete plans.

Next Review Date

The date on which this entry should next be reviewed (at the latest).

The Risk Response Section should only be completed once the risk manager, with input from other appropriate team members, determines the risk warrants the development of a response.

Risk Response Type

The type of risk response. This will have a value of *Avoidance, Mitigation* or *Acceptance*.

Risk Response Plan

The plan developed for handling the risk, dependent on the risk type.

Revised Exposure

The new exposure value should the risk response plan be implemented.

Trigger Event

The event that will occur that acts as a trigger for the start of the response plan.

Start Date

Once the risk response plan begins implementation, this is the date that it started.

Assigned To

The name of the person responsible for developing the risk response plan and for implementing or monitoring its implementation.

Status

The status of the risk response. It will have the following values

- Assessed – an identified risk currently with no risk response plan
- Planned – an identified risk with a risk response plan
- In Process – a risk with risk control in progress (the response plan is being implemented)
- Closed – a risk that has been closed

% Complete

The percent complete for a response plan that has started.

Due Date

The date the execution of the response plan should complete.

Completion Date

The actual date the execution of the response plan completed.

Appendix B – Risk Report

Usage

The Risk Report is a summary of information from the Risk Form. It is meant to allow the quick viewing of all risks that have been identified.

The records on the Risk Report are sorted by Project Name (ascending) then Exposure (descending).

Field Descriptions

Ref

Reference number is an automatically generated numeric field sequentially assigned to each risk.

Entry Date

The date the risk record was created.

Submitter

Name of the person who submitted the risk.

Project Name

Name of the project with which the risk is associated.

Title

Title of the risk used as a short reference.

Exposure

The result of the probability factor multiplied by the impact factor. Value of less than 1 is low/be aware, 1.0 - 2.5 is monitor carefully / outline plans, 5.0 - 10 is monitor closely / complete plans.

Risk Response Type

The type of risk response. This will have a value of *Avoidance*, *Mitigation* or *Acceptance*.

Risk Response Plan

The plan developed for handling the risk, dependent on the risk type.

Revised Exposure

The new exposure value should the risk response plan be implemented.

Trigger Event

The event that will occur that acts as a trigger for the start of the response plan.

Start Date

Once the risk response plan begins implementation, this is the date that it started.

Assigned To

The name of the person responsible for developing the risk response plan and for implementing or monitoring its implementation.

Status

The status of the risk response. It will have the following values

- Assessed – an identified risk currently with no risk response plan
- Planned – an identified risk with a risk response plan
- In Process – a risk with risk control in progress (the response plan is being implemented)
- Closed – a risk that has been closed

% Complete

The percent complete for a response plan that has started.

Due Date

The date the execution of the response plan should complete.

Completion Date

The actual date the execution of the response plan completed.

Next Review Date

The date on which this entry should next be reviewed (at the latest).