Company_Name

Project_Name

Test_Phase Test Plan

Version 1.0

Version_Date

Table of Contents

Table of Tables

1. Introduction

1.1. Using This Template

Stop – Read This First!!!

Before you begin filling out information in this template, first update the document codes that are embedded throughout this template (this will save you time). Go to File, Properties and then go to the Custom tab. You'll see the following entries – just update them with information pertinent to your project:

- Project – Project Name
- Company – Company Name
- Version – Version number of this document
- VersionDate – The date this version was published

Delete this portion (Section 1.1) once you've completed your version of the document.

Please go to CarnegieQuality.com for questions or comments on this template.

1.2. Purpose

The purpose of this plan is to document policies and procedures for identifying and handling uncommon causes of project variation (i.e. risk). Risk should be thought of as the possibility of suffering a negative impact to the project, whether it be decreased quality, increased cost, delayed completion, or project failure.

1.3. Intended Audience

Describe the intended audience of this plan. Generally, the risk management plan should apply to everyone on the project, including any consulting/contractor teams or resources.

1.4. Risk Management Approach

The overall risk management approach follows the standard risk management model as show in the following diagram.

1.4.1. Risk Identification

During risk identification, the sources of risk, potential risk events, and symptoms of risk are identified – refer to Section 3 for details.

1.4.2. Risk Analysis

During risk analysis, the value of opportunities to pursue vs. the threats to avoid, and the opportunities to ignore vs. the threats to accept are assessed – refer to Section 4 for details.

1.4.3. Response Planning

During response planning, risk management and contingency plans are developed – refer to Section 5 for details.

1.4.4. Risk Monitoring and Control

During risk monitoring and control, corrective action plans are developed, implemented, and monitored – see section 6 for details.

1.5. Revision History

Revision	Author	Date	Comments
1.0	Brad Kuhn	06/11/2007	Template

2. Roles and Responsibilities

For each project role, describe the responsibilities in regards to risk. Some representative roles and responsibilities are defined below in the template – these should be added to and tailored for your respective organization/project.

2.1. Project Manager

The project manager is responsible for approval of the risk management plan (this document), leads and participates in the risk management process, and takes ownership of risk mitigation/contingency planning and execution. The project manager is ultimately responsible for the final decision on risk actions, in coordination with the project sponsors.

2.2. Project Team

Project team members (analysts/product managers, developers, testers, and deployment team members) participate in the risk identification process and discuss risk monitoring and mitigation activities at team meetings.

2.3. Software Quality Assurance Lead

The software quality assurance (SQA) lead is responsible for ensuring identified risks are being managed per the risk management plan. The SQA lead also assist in identifying new risks and/or proposing mitigation strategies and contingency plans, along with proposing improvements to the risk management plan and processes.

2.4. Project Sponsors

Project sponsors participate in risk identification and risk activities, as necessary. Project sponsors also receive escalated risks and assist with mitigation and contingency actions for escalated risks.

2.5. Project Stakeholders

Stakeholders assist in monitoring risk action effectiveness and participate in risk escalation, as necessary.

3. Risk Identification

This section contains sample content which should be adapted to your specific project.

3.1. Background

During risk identification potential sources of risk and potential risk events are developed. Section 7.1 shows a sample risk categorization. Pre-defined risk categories provide a structure that helps to ensure that a systematic process is followed to identify risks. Risk categories can be tailored over time, as specific projects demand (additions to risk categories should be maintained in this document for use in future projects). After identifying and categorizing the risk event, it is entered into the risk register.

3.2. Sources

Risk identification is done throughout the life-cycles of a project, although a majority of the risks should be identified early on so proper response planning and monitoring can occur. The following should be considered as tools and techniques for risk identification:

- Analysis of high-level deliverables
- Analysis of the WBS and project schedule
- Analysis of scope change requests
- Analysis of project assumptions
- Project team input (which can take the form of interviews, brainstorming sessions, and/or Delphi technique)
- Stakeholder and sponsor input
- Formal risk identification sessions
- Previous lessons learned
- SQA audits and reviews
- Performance and status reports
- Diagramming techniques such as cause and effect diagrams, process or system flows, and influence diagrams.

3.3. Documentation

All identified risks should be documented and entered into the risk register (an Excel spreadsheet), which is kept <list location here>. During risk identification, the following information is required for documentation:

- Risk category
- Risk trigger
- Potential outcome

- Raised By
- Date Raised
- Source

The risk trigger is the event that would need to happen in order for the potential outcome to occur. Risk triggers are usually expressed with some sort of dependency, or qualifier. For example, a risk trigger might be that a resource on the project leaves. This might easily be accounted for by utilizing other resources. But if a resource with key skills or knowledge leaves, then the project may be significantly impacted. This approach is suggested in order to clarify the thought process of identifying risks. When the risk trigger occurs, the risk is no longer a risk, but has materialized into a problem/issue that needs resolution.

4. Risk Analysis

This section contains sample content which should be adapted to your specific project.

4.1. Background

After a risk or group of risks has been identified and documented, risk analysis should be performed. During risk analysis, each potential risk event is analyzed for:

- The probability that the risk will occur
- The impact of the risk if it occurs

Risk probabilities are defined in Section 7.2 of the Appendix. Risk impact definitions are defined in Section 7.3 of the Appendix. Impacts can be assessed against project cost, schedule, scope, and/or quality. If the risk event affects more than one dimension and the scores are different, the higher impact definition should be utilized.

Once the appropriate risk impact and probability are selected, the risk score can be determined. The risk probability and impact matrix is shown in section 7.5 of the Appendix. The matrix shows the combination of impact and probability that in turn yield a risk priority (shown by the red, yellow, and green colored shadings).

Risk priority is utilized during response planning and risk monitoring/control (see Sections 5 and 6). It is critical to understand the priority for each risk as it allows the project team to properly understand the relative importance of each risk.

Risk impact analysis can be qualitative or quantitative.

4.1.1. Qualitative Analysis

Qualitative analysis is a quicker and usually more cost-effective way to analysis risks (as opposed to quantitative analysis). Analysis should be performed with the goal of gathering data on:

- The likelihood of the risk occurring (using definitions from Section 7.2)
- The qualitative impact on the project (using definitions from Section 7.3)
- The quality of the risk data being utilized (e.g. how reliable is the data?)

4.1.2. Quantitative Analysis

Quantitative analysis utilizes techniques such as simulation and decision tree analysis to provide data on:

- The impact to cost or schedule for risks
- The probability of meeting project cost and/or schedule targets
- Realistic project targets on cost, schedule, and/or scope

Qualitative analysis should occur prior to conducting quantitative analysis. Not every risk needs to go through quantitative analysis. If quantitative analysis is to be used, then this section should contain information on:

- Defined criteria for which risks go through quantitative analysis
- Technique(s) to be utilized
- Expected outputs of quantitative analysis

4.2. Documentation

The results of risk analysis should be documented in the risk register. The following information shall be entered in the register:

- Risk impact
- Risk probability
- Risk matrix score – computed by the risk register spreadsheet after impact and probability are entered
- Risk priority – computed by the risk register spreadsheet after impact and probability are entered
- Qualitative impact – descriptive comments about the potential risk impact

5. Response Planning

This section contains sample content which should be adapted to your specific project.

5.1. Background

During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed. Higher priority risks should receive more attention during response planning than lower priority risks. Every risk threat should be assigned an owner during response planning.

5.2. Risk Strategies

There are several methods for responding to risks.

5.2.1. Avoid

Risk avoidance involves changing aspects of the overall project management plan to eliminate the threat, isolating project objective's from the risk's impact, or relaxing the objectives that are in threatened (e.g. extending the schedule or reducing the scope). Risks that are identified early in the project can be avoided by clarifying requirements, obtaining more information, improving communications, or obtaining expertise.

5.2.2. Transfer

Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat, it simply makes another party responsible for managing it.

5.2.3. Mitigate

Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.

5.2.4. Accept

Acceptance is often taken as a risk strategy since it is very difficult to plan responses for every identified risk. Risk acceptance should normally only be taken for low-priority risks (see Section 4.1). Risk acceptance can be passive, where no action is taken at all, or active. The most common active approach to risk acceptance is to develop a cost and/or schedule reserve to accommodate known (or unknown) threats.

5.3. Documentation

The results of response planning should be documented in the risk register. The following information shall be entered in the register:

- Response strategy (avoid, transfer, mitigate, or accept)

- Response notes (description of plan) – if a mitigation approach is taken, specific trigger points that require aspects of the contingency plan to be executed should be documented
- Risk owner

6. Risk Monitoring and Control

This section contains sample content which should be adapted to your specific project.

6.1. Background

Planned risk responses (see Section 5) should be executed as required over the life-cycle of the project, but the project should also be continuously monitored for new and changing risks. During risk monitoring and control the following tasks are performed:

- Identify, analyze, and plan for new risks
- Keep track of identified risks and monitor trigger conditions
- Review project performance information (such as progress/status reports, issues, and corrective actions)
- Re-analyze existing risks to see if the probability, impact, or proper response plan has changed
- Review the execution of risk responses and analyze their effectiveness
- Ensure proper risk management policies and procedures are being utilized

6.2. Timing

Discuss how often the risk monitoring and control process will occur over the lifetime of the project.

6.3. Documentation

The results of risk monitoring and control should be documented in the risk register. The following information shall be entered in the register:

- Status – valid statuses are:
    - Identified – Risk documented, but analysis not performed
    - Analysis Complete – Risk analysis done, but response planning not performed
    - Planning Complete – Response planning complete
    - Triggered – Risk trigger has occurred and threat has been realized
    - Resolved – Realized risk has been contained
    - Retired – Identified risk no longer requires active monitoring (e.g. risk trigger has passed)
- Trigger Date – if the risk has been triggered
- Notes

7. Appendix A: Definitions

Each appendix contains sample content which should be adapted to your specific project.

7.1. Risk Categories

The following diagram shows pre-defined risk categories. Risk categories should be used in thinking about and identifying risks (see Section 3 for more details).

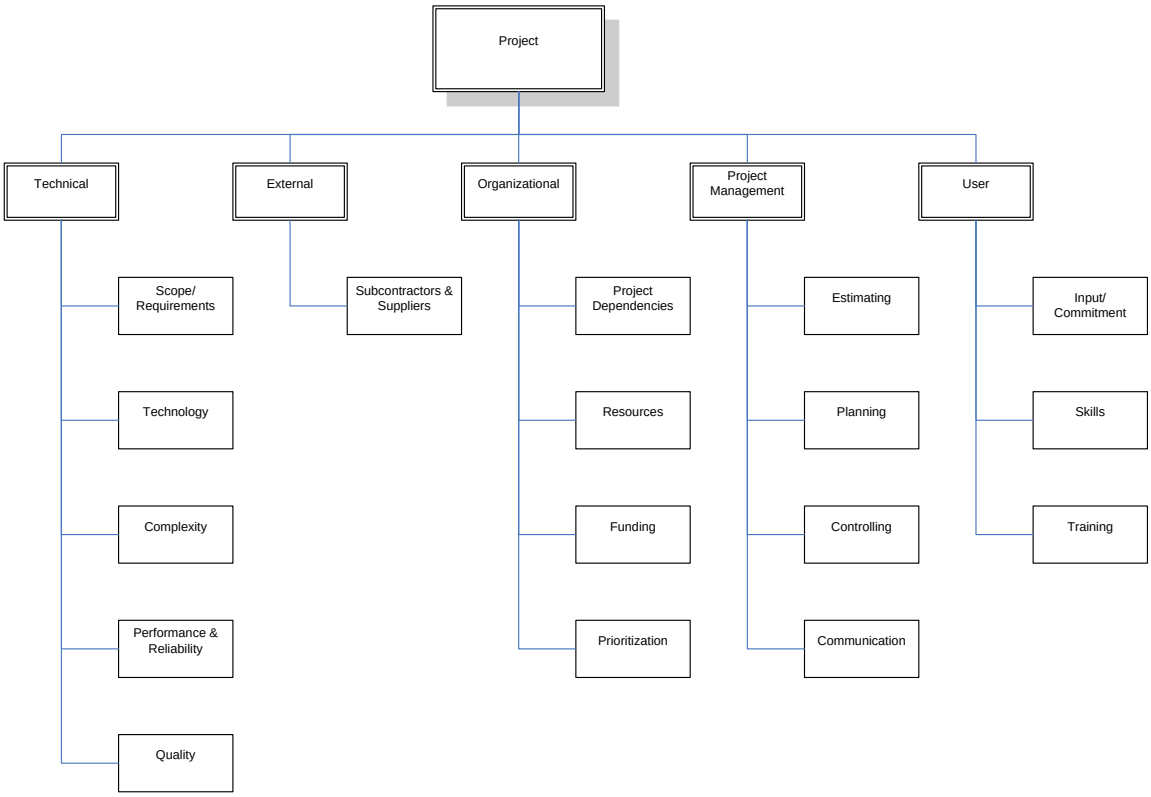

Table 1 – Risk Categories

7.2. Risk Probability Definitions

The following chart shows risk probability definitions. During risk analysis the potential likelihood that a given risk will occur is assessed, and an appropriate risk probability is selected from the chart below (see Section 4 for more details).

Probability Category	Probability	Description
Very High	0.90	Risk event expected to occur
High	0.70	Risk event more likely than not to occur
Probable	0.50	Risk event may or may not occur
Low	0.30	Risk event less likely than not to occur
Very Low	0.10	Risk event not expected to occur

Table 2 – Risk Probability Definitions

7.3. Risk Impact Definitions

The following chart shows risk impact definitions across each of the potentially impacted project areas (cost, schedule, scope, and quality). During risk analysis the potential impact of each risk is analyzed, and an appropriate impact level (0.05, 0.10. 0.20, 0.40, or 0.80) is selected from the chart below (see Section 4 for more details).

Project Objective	Very Low 0.05	Low 0.10	Moderate 0.20	High 0.40	Very High 0.80
Cost	Insignificant cost impact	< 10% cost impact	10-20% cost impact	20-40% cost impact	> 40% cost impact
Schedule	Insignificant schedule impact	< 5% schedule impact	5-10% schedule impact	10-20% schedule impact	> 20% schedule impact
Scope	Barely noticeable	Minor areas impacted	Major areas impacted	Changes unacceptable to sponsor	Product becomes effectively useless
Quality	Barely noticeable	Only very demanding applications impacted	Sponsor must approve quality reduction	Quality reduction unacceptable to sponsor	Product becomes effectively useless

Table 3 – Definition of Risk Impact Scales

7.4. Risk Probability and Impact Matrix

The risk probability and impact matrix shows the combination of risk impact and probability, and is utilized to decide the relative priority of risks. Risks that fall into the red-shaded cells of the matrix are the highest priority, and should receive the majority of risk management resources during response planning and risk monitoring/control. Risks that fall into the yellow-shaded cells of the matrix are the next highest priority, followed by risks that fall into the green-shaded cells.

Probability	**Threats**				
0.90	0.05	0.09	0.18	0.36	0.72
0.70	0.04	0.07	0.14	0.28	0.56
0.50	0.03	0.05	0.10	0.20	0.40
0.30	0.02	0.03	0.06	0.12	0.24
0.10	0.01	0.01	0.02	0.04	0.08
	0.05	0.10	0.20	0.40	0.80

Table 4 – Risk Probability and Impact Matrix