
Notes on accessibility: This document has been tested and is best accessible with JAWS 11.0 or higher.



Centers for Medicare & Medicaid Services CMS eXpedited Life Cycle (XLC)

XLC Risk Management Guidance and Risk Register Instructions

Version 2

05/30/2014

Document Number: <document's configuration item control number>

Contact Number: <current contract number of company maintaining document>

Table of Contents

Table of Contents	i
List of Figures	ii
List of Tables	ii
Introduction	1
1.1 Background	1
1.2 Purpose	1
1.3 Risk Management Approach	1
1.4 Risks	2
1.5 Roles and Responsibilities	2
1.5.1 Key Risk Management Team	2
Procedure	4
1.6 Scope	4
1.7 Definitions	4
1.8 Risk Definition	4
1.9 Risk Management Process	5
1.9.1 Step 1 - Risk Management Planning	6
1.9.2 Step 2 - Risk Identification	9
1.9.3 Steps 3 & 4 - Risk Analysis (Qualification & Quantification)	13
1.9.4 Step 5 - Risk Mitigation Planning	21
1.9.5 Step 6 – Risk Tracking	25
1.9.6 Conduct Project-Level Risk Status Meetings	25
1.9.7 Validate Team-Level Attention to RM	25
1.9.8 Emphasize Risk throughout the Project Lifecycle	26
1.9.9 Communicate Risks	26
1.9.10 Escalate Risks	26
1.9.11 Initiate More Oversight for Tasks with High Risk	26
1.9.12 Conduct Risk Audits	27
Appendix A: Acronym List	28
Appendix B: Risk Identification (Step 2) Techniques Descriptions	29
Appendix C: Risk Register Template	35
Acronyms	40
Glossary	41
Related Documents	42
Revision History	43

Approvals.....	44
-----------------------	-----------

List of Figures

Figure 1. Risk Management Process	6
Figure 2. Risk Breakdown Structure - Example.....	32

List of Tables

Table 1. Risk Management Team	3
Table 2. Risk Statements - Examples	5
Table 3. Risks and Triggers - Example	12
Table 4. Risk Register Template - Step 2 – Risk Identification.....	12
Table 5. Risk Register Data Elements for Step 2 – Risk Identification	12
Table 6. Risk Exposure Rating.....	15
Table 7. Risk Matrix.....	15
Table 8. Probability of Occurrence Rating.....	15
Table 9. Ratings and Types of Impact Criteria	16
Table 10. Ratings for Trigger Event Date Timeframe.....	18
Table 11. Top 5 Risk List.....	19
Table 12. Risk Register Template – Steps 3 & 4, Risk Analysis (Quantitative and Qualitative).....	19
Table 13. Risk Register Data Elements for Steps 3 & 4 - Risk Analysis (Qualification & Quantification).....	20
Table 14. Risk Response Matrix	23
Table 15. Risk Register Template – Step 5 – Risk Mitigation Planning.....	24
Table 16. Risk Register Data Elements for Step 5 – Risk Mitigation Planning	24
Table 17. Risk Register Template – Step 6 – Risk Tracking	27

Table 18. Risk Register Data Elements for Steps 6 – Risk Tracking.....	27
Table 19. Acronym List.....	28
Figure 2. Risk Breakdown Structure - Example.....	32
Table 20. List of Acronyms.....	40
Table 21. Glossary	41
Table 22. Related Documents.....	42
Table 23. Revision History	43

1. Introduction

Risk management (RM) gets at the heart of effective communication, which is a significant part of project management. A successful RM program is one in which risks and opportunities are continuously identified, analyzed, prioritized, responded to, tracked, and controlled effectively using project resources.

When project teams and their management focus on the discipline of RM and incorporate it into project planning and execution, project success usually follows because issues (i.e., risks that are realized) are prevented before they occur and opportunities are identified to improve technical, cost, schedule, or quality performance of the project.

The objective of a well-managed RM program is to provide a repeatable process for balancing cost, schedule, and performance goals within project funding, especially on projects with designs that approach or exceed the state-of-the-art or have tightly constrained or optimistic cost, schedule, and performance goals.

1.1 Background

RM is a continuous process that is accomplished throughout the project. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective RM depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

Project RM is not a stand-alone Project Management Office (PMO) task. It is supported by a number of other project office tasks. In turn, the results of RM are used to finalize those tasks. Important tasks, which must be integrated as part of the RM process, include: requirements development, logical solution and design solution (systems engineering), schedule development, performance measurement, Earned Value Management (EVM) (when implemented), and cost estimating. Planning a good RM program integral to the overall project management process ensures risks are handled at the appropriate management level. Emphasis on RM coincides with overall Centers for Medicare & Medicaid Services' (CMS) efforts to reduce life cycle costs (LCC). New processes, reforms, and initiatives are being implemented with RM as a key component. It is essential that projects define, implement and document an appropriate RM and mitigation approach. RM should be designed to enhance project management effectiveness and provide Project Managers (PMs) with a key tool to reduce LCC, increase project likelihood of success, and assess areas of cost uncertainty.

1.2 Purpose

The purpose of this procedure is to provide guidance to successfully implement and effectively manage project risk within CMS.

1.3 Risk Management Approach

Figure 1 (shown on page 6) depicts the RM process that will be used. RM is a multidisciplinary process. Risks will be identified by anyone on the project team at any time. RM is iterative and shall be performed throughout the project lifecycle. Focused attention to risk identification

should occur prior to each milestone or gate review followed by continuous review and management of risks throughout the project life cycle.

A major objective of RM is to quickly and accurately:

- Recognize and record the risk.
- Analyze the risk(s) using RM tools presented in Appendix C (Risk Register). The [Risk Register](#) can be downloaded from the CMS website.
- Discuss the risk with the appropriate level of decision makers in the project.
- Develop and approve appropriate risk response plans for each high priority risk within one to two weeks of finishing risk analysis.

1.4 Risks

Without effective RM processes and procedures:

- Risks may not be comprehensively identified, reviewed and/or mitigated.
- The PMO may find itself doing crisis management, a resource-intensive process that is typically constrained by a restricted set of available options.

Successful RM depends on knowledge gleaned from assessments of all aspects of the project coupled with appropriate mitigations applied to the specific root causes.

1.5 Roles and Responsibilities

RM activities involve everyone on the project, including project stakeholders who will be involved in varying degrees depending on the stage of the project. The PM is responsible for designating roles and responsibilities related to the specific project-level RM activities.

1.5.1 Key Risk Management Team

- **Project Manager:** Accountable for RM planning and ensuring the process is implemented and followed. The PM will assign a Risk Manager/Coordinator to the project, and identify this individual on the project's organization chart. The PM will be involved in the initial risk identification, analysis, and risk response activities and then focus more on monitoring and control.
- **Risk Manager/Coordinator:** Accountable to the PM and acts on the PM's behalf for managing and coordinating the RM activities on the project. This function may be performed by the PM based on the size and complexity of the project.
- **Project Sponsor:** Responsible for realization of project benefits and should be involved in the RM process, especially at the start, when it is important to understand the challenges the project faces. The sponsor will be invited to risk activities at regularly scheduled intervals throughout the project life cycle.
- **Business Subject Matter Expert (BSME):** Assists in identifying and determining the context, consequence, impact, timing, and priority of the risk.

In addition to the Key RM Team roles, the following roles are integral to RM:

- **Stakeholder(s):** Responsible for bringing unique perspectives to risk identification analysis, mitigation planning and staying involved in the risk tracking activities. They

assist in identifying and determining the context, consequence, impact, timing, and priority of the risk. They will be invited to risk activities, as required, and risk owners will involve them in risk mitigation planning.

- **Project Team:** Responsible for identifying and analyzing risks. Some team members will be assigned as Risk Owners and will be responsible for risk mitigation planning and tracking.
- **Risk Owner(s):** Responsible for managing the risk assigned by the PM or Risk Manager/ Coordinator. Their primary responsibility is to develop mitigation, contingency, and fallback plans, perform the steps of the mitigation plan and report progress to the Risk Manager/ Coordinator. The Risk Owner will ensure the documentation on the assigned risk(s) is accurate and obtain enough supporting information for analysis to ensure the risk(s) is/are understood and properly prioritized.

Table 1 provides an example that can be used to identify the RM Team membership.

Table 1. Risk Management Team

Role	Assigned	Organization	Email	Phone
Project Manager (PM)				
Risk Manager/Coordinator				
Project Sponsor				
Stakeholder(s)				
Risk Owner(s)				

2. Procedure

2.1 Scope

This Guidance provides a step-by-step approach to RM that can be tailored to fit specific project needs. This core project management practice includes processes and techniques and provides templates for managing risks associated with the entire project lifecycle. The RM process focuses on risks that affect the project as a whole as well as the risks associated with the major Work Breakdown Structure (WBS) Level 1 tasks.

2.2 Definitions

Risks can be identified by anyone on a project at any point in the lifecycle. It is a multidisciplinary process. However, extra time should be taken during the development of the Business Case during Acquisition Planning to identify potential risks to the project. Concentrated focus on risk identification is critical at the beginning of the project execution phase followed by continuous review and management of risks throughout the entire lifecycle.

Risk and issue identification, as well as the actions taken in response to these, are critical to the success of a project. It is important to clarify the terms "Risk," "Issue," and "Action Item". All three are very different in both their impact on the project as well as the time and resources required to manage them.

- **Risk:** A measure of future uncertainties in achieving project performance goals and objectives within defined cost, schedule, and performance constraints. Risk can be associated with all aspects of a project (e.g., threat, technology, maturity, supplier capability, design maturation, performance against plan) as these aspects relate across the WBS and Integrated Master Schedule (IMS). Risks have three components: 1.) A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring; 2.) a probability (or likelihood) assessed at the present time of that future root cause occurring; 3.) a consequence (or effect) of that future occurrence. (Source: Risk Management Guide for DoD Acquisition, Sixth Edition)
- **Issue:** A risk that has been realized. Issues require immediate resolution and, if left unresolved, will negatively impact the project. An issue may also emerge that was totally unforeseen and unrecognized as a risk, and therefore must be addressed immediately. This should be considered the exception and not the norm once RM is fully implemented.
- **Action Item:** An activity that has a finite resolution and timeframe for completion and can be performed within the current scope of the project (i.e., the activity can be performed within the existing schedule and budget, with existing resources). An action item can also be thought of as an activity that needs to be performed in support of the project or task. Typically an "Action Item" can be resolved quickly; however, if left unresolved the action item could become a risk.

2.3 Risk Definition

Risks defined early form a baseline to initiate RM activities, but they must be defined with enough detail that those assigned to respond to the risk and others external to the project can fully understand the risk. The main objective is to find the significant risks associated with the project. Identification of "schedule" or "cost" as risks is not acceptable, because these alone are

not risks. Finding the specific source of the risk that leads to a negative project result is key to mitigating risks. Risks must be defined in sufficient detail so that impact and probability analysis on each risk can be effectively assessed. A risk statement consists of a:

- **Condition/Cause** or situation that currently exists - the circumstances that are causing concern for a potential loss to the project.
- **Risk Event** that could trigger a negative result - the event or situation that will potentially happen and could trigger a negative result.
- **Effect or Impact** - the consequence or outcome which impacts project objectives related to cost, time, scope, quality, and customer satisfaction.

An example of a risk statement is: "Because of (*condition/cause*), there is a possibility that (*risk event*) will result in (*effect/impact*). Table 2 provides some examples of risk statements.

Table 2. Risk Statements - Examples

Risk	Condition/Cause	Risk Event	Effect or Impact
1	As the result of choosing a specific COTS or GOTS products,	If, qualified staff with required skills are not available during the design phase;	This may result in extending the design stage by four months.
2	Release 2.0 was not designed to scale beyond 150 users,	If, management makes the decision to expand this release to 500 users,	Release 2.0 could completely halt resulting in users going back to the old system damaging our reputation and chance for future funding?
3	There is only two days scheduled for performance load testing on the system,	If adequate testing cannot be done before deployment, then	Queries will take too long to complete, users will not accept the system, and subsequent releases may not be funded.

Opportunities associated with a project can have a positive effect on that project and must be managed as risks. As a PM looks at responses to high priority risks, it is possible not only to minimize their influence, but to take advantage of opportunities as well. For example, a PM may spend funds to bring in a very experienced developer for a critical component of a software interface to limit the number of defects and gain some time in the schedule. The PM could leverage this person's expertise (make the most of an opportunity) during this time to work on other areas of the project as well.

2.4 Risk Management Process

The RM process Model includes the following steps: Risk Management Planning, Risk Identification, Risk Analysis (both Qualification and Quantification), Risk Mitigation Planning, and Risk Tracking performed on a continuous basis. Figure 1 on page 6 graphically depicts this continuous process which requires continuous management by all Risk Management Team participants (Stakeholders and Management).

Figure 1. Risk Management Process



Each Step of the Risk Management Process Model will be discussed in detail below:

2.4.1 Step 1 - Risk Management Planning

The first, often-overlooked step in RM is Risk Management Planning. It is important for PMs to actively plan how they want to implement a formal RM process. Without concrete planning and a committed effort to RM, the project will follow the standard informal approach where the PM uses intuition, experience, and expertise to minimize and handle problems that could derail the project.

In contrast, mature project management includes a proactive approach to managing risk. This allows teams to focus on the solution and less time responding to problems that could be eliminated or minimized if proactive steps were taken earlier in the project.

Once an approach to RM has been established, it should be documented in a Risk Management Plan. A template for a [Risk Management Plan](#) is on the CMS website.

The specific steps to Risk Management Planning include defining the:

- Project-specific approach to RM
- Roles and responsibilities
- Project RM activities

2.4.1.1 Define Project-Specific Approach to RM

Each project is unique. Therefore RM should be tailored accordingly to meet the specific needs of the project. Projects can choose to implement RM "as is" or alter it based on their experience or the project complexity. At a minimum, the PM needs to make decisions on:

- 1) RM process steps
- 2) Roles and responsibilities, as well as level of involvement from each Project Team member, team leader, stakeholders, project sponsor, executive management and other projects
- 3) Process to engage stakeholders in RM
- 4) Type and frequency of RM activities to identify, analyze, respond to and monitor risks
- 5) Types of risk rating schemes to use for qualitative analysis
- 6) Tools, repositories (Risk Register), or templates to capture, analyze, monitor, manage, and control risks identified.

2.4.1.2 Define Roles and Responsibilities

The PM is responsible for the project delivery, but the Sponsor – the one who funds the effort and has the responsibility for the realization of the benefits – must be actively involved in the RM process. Executive, senior and middle management teams and key Stakeholders have roles as well. Open discussion about risks, mistakes, or potentially damaging information is required for RM to be effective in supporting informed decision-making.

The PM, Project Sponsor, and the Project Team are the typical participants in the formal RM process. If the project is complex, highly visible or above the organization's threshold in more than one criteria, then the Project Sponsor and key Stakeholders should be involved in the RM process.

The PM is responsible for designating the roles and responsibilities of the participants in the RM activities. Typically the roles are:

- **Project Manager:** accountable for RM planning and ensuring the process is implemented and followed.
- **Project Sponsor:** responsible for realization of project benefits and should be involved in the RM process, especially at the start, when it is important to understand the challenges the project faces. The Sponsor should also be involved at regularly scheduled intervals throughout the project lifecycle.
- **Stakeholders:** responsible for bringing unique perspectives to risk identification analysis and response planning and staying involved in the risk monitoring activities.
- **Team:** responsible for identifying and analyzing risks. Some team members will be assigned as risk owners and will be responsible for risk response planning and monitoring.

- **Risk Owner:** responsible for managing the risk assigned. The owner ensures the documentation is completed accurately and manages the process to obtain enough supporting information in order to move to risk analysis where the risks are prioritized. The Risk Owner's primary responsibility is to develop mitigation, contingency, and fallback plans.

One of the jobs of the PM is to promote the idea that everyone is a Risk Manager (i.e., employees take responsibility for their actions and outcomes) and create an environment where team members, the Project Sponsor, Key Stakeholders, Subject Matter Experts (SME), other PMs, end users, and outside experts aid in the risk identification process. This facilitates capturing risks more quickly and accurately.

The test of a strong RM program is how quickly and how accurately the following happens:

- The risk is recognized
- The risk is recorded in the RM system
- The risk makes it to the appropriate decision-making level in the project
- An appropriate risk mitigation strategy is determined and jointly agreed upon.

Stakeholders are also important in the RM process. Since each Stakeholder brings a unique perspective to the identification and response to risk based on their role and responsibilities at different points in the lifecycle, it is imperative that they are involved throughout the project.

2.4.1.3 Define the Project RM Activities

Scheduling at least one formal RM activity to address each step in the process is an easy way to implement and incorporate RM into the Project. Once a team experiences these activities initially, the iterative continuous approach to RM begins, the benefits of RM become apparent, and risk activities become integrated into project procedures. Risk activities for each step in the process are described below.

- **Step 1: Risk Management Planning** - After formalizing the RM approach:
 - Define the type and frequency of risk/issue and project status meetings. For complex projects, it is recommended that the PM hold a formal "Risk/Issue Meeting"... weekly or every other week. This meeting should include the Team, Sponsor, and Key Stakeholders. If the project schedule is aggressive or the scope or cost management is challenging, it is important to hold these meetings regularly.
 - Schedule a team meeting to explain the RM project culture (e.g., everyone is responsible for risk), RM process, roles and responsibilities, expectations, risk status meetings format and frequency, and tools.
- **Step 2: Risk Identification** - Pick one or several identification technique(s) and conduct one or several sessions to identify and define risks and opportunities for the project.
- **Steps 3 & 4: Risk Analysis** - Pick one or several techniques to analyze risks with the objective to produce a prioritized list - a "Top 5 Risk List."
- **Step 5: Risk Mitigation Planning** - Make sure Risk Owners are assigned to high-priority ("Top 5 Risk List") risks and give them the time to develop Mitigation, Contingency and Fallback Plans. Create a Risk Response Matrix and ensure that plans are developed, accurate, reasonable, and cost-effective.

- **Step 6: Risk Tracking** - This step ensures the entire RM process is working as planned and involves coordination, planning and reporting of risk status, priorities, responses, assignments, as well as the management of any issues that may have risen.

2.4.2 Step 2 - Risk Identification

Risk Identification involves determining the risk events or opportunities that are likely to affect the project, then classifying them according to their cause or source.

- Risk is an uncertain event or condition that, if it occurs in the future, may impact the project's objectives negatively or positively.
- A risk that can potentially impact the project negatively is classified as a "Threat."
- A risk that can potentially impact the project positively is classified as an "Opportunity."

While most PMs concentrate on "Threats" to their projects, it is also helpful to identify "Opportunities" because they may provide extra benefits to the project if managed appropriately.

The identification process should be conducted early and often in an organized and thorough manner designed to uncover a large number of potential risks to a project. PMs who do not spend time and resources to identify, analyze, and respond to risks early in the project lifecycle will likely pay a greater cost later when they find themselves reacting to a problem when it occurs.

Although Risk Identification should be comprehensive, it does not mean identifying every probable scenario of unlikely events. The process includes identifying the most significant risks to the project as a whole, as well as the risks associated with individual tasks. One task, especially one that falls on the critical path, could easily delay project delivery.

On projects where it is understood that everyone is a Risk Manager, after the first formal sessions to identify risk, informal "coffee pot" discussion sessions often become the source of new risks or changes to risk responses. It is important to document these informal sessions so findings are not lost. In addition, informal discussions should not take the place of regularly scheduled risk meetings where formal status is captured.

IMPORTANT: Do not analyze the risks during Risk Identification; just capture as much information as possible in order to clearly define the risk. Worry about characteristics of the risk later during the Risk Analysis, Steps 3 & 4.

2.4.2.1 Identify Sources of Risk

Organizing risks by standard categories that are relevant for your project facilitates better management throughout the project lifecycle. Such an approach often uncovers additional risks.

Sources of risk can be in the form of categories of possible risk events that may affect the project positively or negatively; or can be derived from internal project documentation or the experience of the Project Team and Stakeholders. There is significant information about sources of risk in published project management literature, other government risk management plans, and commercially available materials. Some of these materials are in the form of risk checklists, risk breakdown structures, or taxonomies - all of which are described in the subsequent subsections. Risk sources are generally categorized as external or internal:

External Risks - those that originate outside the control of the project team. These include:

- Political

- Policy or Legislative
- Funding
- Environmental
- Stakeholder

Internal Risks - those that the team can influence through effective management practices, processes, and decisions related to cost, schedule, performance and technology approaches. These include:

- Requirements
- Technology
- Cost
- Schedule
- Resources
- Programmatic

IMPORTANT: Use categories with caution. A PM should always remain open to consider risks that fall outside these categories, especially since this is an information gathering step where all input is considered.

2.4.2.2 Uncover OMB 300 Specific Risk

The Federal Government must effectively manage its portfolio of capital assets to ensure that scarce public resources are wisely invested. As part of this management process, the Office of Management and Budget (OMB) requires a report on Information Technology (IT) (i.e., OMB Circular A-11, Exhibit 53). This includes an Exhibit 300 that includes information on plans, justifications, and risks for major acquisitions as identified in OMB Circular A-11. For all investments, both IT and non-IT, an Agency must discuss the risks, including plans with milestones and completion dates to eliminate, mitigate, or manage the risk.

2.4.2.3 Uncover Project Risks Using Identification Techniques

There are a variety of techniques used by industry risk experts to identify project risks. A few of these are listed below with a short description of each technique. The top five on this list are the suggested because they are both effective and easy to execute.

PMs can use one or many of the risk identification techniques listed below. The method chosen is based on the management style and experience of the PM and the dynamics of the team. Remember, project management is both an art and a science, so if one technique doesn't work, try another.

The techniques for identifying risks are:

1. Brainstorming
2. Structured Reviews
3. Sticky Notes
4. Affinity Diagrams
5. Checklists
6. Risk Breakdown Structure (RBS)

7. Assumption and Constraint Analysis
8. Taxonomies
9. Expert Interviews
10. Strengths, Weaknesses, Opportunities, Threats (SWOT) Analysis
11. Lessons Learned
12. Delphi Technique

Appendix B contains descriptions of each of the above Risk Identification Technique.

2.4.2.4 Assign Risk Owners

At this step, either one person is assigned as a Risk Owner or individual team members are assigned to document each risk identified. It is important to capture as much information as possible about each risk before moving forward to the analysis phase. When risks are analyzed and it is time to create risk mitigation plans for the high-priority risks, the PM should assign an individual to manage each risk during the project lifecycle.

This person creates the Mitigation and Contingency Plans and is responsible for managing the risk from the Analysis steps through Tracking. The Risk Owners are not responsible if the risks occur and become issues. They simply document the risk; validate the accuracy of the risk throughout the lifecycle; manage the risk if it does occur; and track the effectiveness of the risk response.

2.4.2.5 Document Risks

Documentation of a risk should include:

- Risk statement: "Because of (condition/cause), the (risk event) will result in (effect/impact).
- Impact to the project and project dependences
- Probability of occurrence
- Impact timeframe for the risk.

PMs will use the Risk Register, see Appendix C, to document and manage the risks identified. The approach chosen will depend on a variety of factors, including the selected risk process, project size, project complexity, project resources, and management expectations.

In the spirit of capturing as much information as possible during the Risk Identification step, it is helpful to identify "Triggers" or early warning signs that a risk has occurred or is about to occur. Triggers are typically identified in the Risk Mitigation step to alert the Project Team to take action as necessary. If known during Risk Identification, "Trigger" information should be captured so it is not forgotten and can be used later during the Analysis steps. Table 3 identifies an example of how to capture Trigger events associated with an identified risk.

Table 3. Risks and Triggers - Example

Risk Statement: Cause, Risk, Effect	Triggers: if known (more fully explain warning signs that the uncertain event or risk is about to happen.)
Overall Project Risk	
If Subject Matter Experts from the business community are not available during the system analysis step, then requirements will likely be inaccurate resulting in an unacceptable solution.	Experts did not attend meeting #1 or #2.

2.4.2.5.1 Risk Register

The Risk Register will be used to document all identified risks which may affect the project. The Risk Register will be accessible by all members of the Risk Management Team including Stakeholders. The Risk Register will ultimately contain the outcomes of the other RM process steps and iterations as they are conducted, resulting in an increase in the level of detail and type of information contained in the Risk Register over time.

Table 4, illustrates the Risk Register Template data elements for Step 2 - Risk Identification:

Table 4. Risk Register Template - Step 2 – Risk Identification

Risk ID	Date Identified	Risk Submitter	Risk Title	Risk Description	Source (Select)	Risk Owner
R001	4-Apr-13	Insert Name	Insert short title	Insert description	Stakeholder	Insert Name

Table 5 identifies information that will be collected and entered into the Risk Register during the Step 2, Risk Identification:

Table 5. Risk Register Data Elements for Step 2 – Risk Identification

Data Element	Description
Risk ID	A unique identifier in a numbering system assigned to a risk. The identifier should be used for reference or for cross-reference in the future among project team members and future project stakeholders in search of historical information. Example: R01, R02, R03...
Date Identified	The original date when the risk was originally brought to light, or identified.

Data Element	Description
	Example: "MM/DD/YY"
Risk Submitter	The name of the individual or group who identified and submitted the risk to bring the attention of project stakeholders.
Risk Title	Short title/description of the risk - No more than 10 words
Risk Description	A brief description of future event that could result in either positive or negative results to the project, and the impact it will have on the project.
Source	Source of risk. Select: Formal Risk Review, Audit/Review, Status Meeting, Stakeholder, Other, as appropriate.
Risk Owner	The individual assigned to the project who tracks the risks for Triggers.

2.4.3 Steps 3 & 4 - Risk Analysis (Qualification & Quantification)

Risk Analysis is the process of reviewing detailed risk data to determine the extent of the risks, how they relate to each other, and which ones are redundant, dependent, and important to highlight. It involves the activities required to prioritize a long list of project risks with the objective to determine which top or critical risks necessitate a response.

Project teams do not need to respond to every risk, especially since resources are typically tight and some risks are not probable or may not have a big impact if they occur.

Teams must perform the analysis necessary to respond to those risks that could gravely impact the project.

Note: Risk Analysis is a snapshot in time and may change significantly during the project. Risk Analysis must be periodically re-accomplished to ensure the analysis remains current.

2.4.3.1 Introduction

Objectives of Risk Analysis vary depending on the phase of the project. When performed during the planning phase, some subjective but important information can be used to make decisions early in a project's lifecycle. For example, if the planned technical approach to use a new vendor appears too risky, the executive team and the PM may make decisions to either cancel the project at this time or modify the approach.

Risk Analysis done in later phases builds upon the earlier work completed and analyzes the risks specific to the work to be performed in order to successfully complete the project.

Risk Analysis includes two types of assessment: risk qualification and risk quantification. These two methods of analysis can be performed separately or together and involve determining the probability of risks and their impacts or consequences to the project.

RM focuses on qualitative analysis. Quantitative analysis involves a labor-intensive effort to examine risk and includes a process of assigning metric values to the high- priority risks, as well as a firm understanding and experience with a repeatable RM process.

2.4.3.2 Analysis - Risk Qualification

Risk Qualification involves several steps to assess the impact and probability of project risks using qualitative terms such as Catastrophic, Very Serious, Serious, Significant, and Marginal. The objective of this analysis is to prioritize those risks that should be managed proactively. The five steps to Risk Qualification are listed below and described in the five subsections that follow.

Step 1: Evaluate Data Accuracy and Comprehensiveness of Risks

Step 2: Conduct General Risk Analysis

Step 3: Determine the Probability and Impact of each Risk

Step 4: Calculate the Risk Score

Step 5: Prioritize the Risks

2.4.3.2.1 Evaluate Data Accuracy and Comprehensiveness of Risks

The Project Team will use the data uncovered in Risk Identification (Step (2)) to analyze risks. Before extensive analysis is done, it is very important that the PM and team leaders conduct a short analysis of the data provided that led to the identification of the risk by asking the questions, "How well do we understand this risk?" or "What led the person to identify the risk in the first place?" or "Can we identify the root cause for this risk?"

The goal is to have enough reliable, accurate data to evaluate the likely risk impact and probability before spending the time and resources to proceed with risk analysis.

2.4.3.2.2 Conduct General Risk Analysis

Analyze risk data to eliminate redundancy; to combine related risks, and to link dependent risks. Ask the standard "who, what, where, when, why, and how" questions related to the risk and try to determine any risk drivers.

Identify the timeframe when the risk may occur. After evaluating the accuracy of the risks on the project risk list, determine what date or where in the project lifecycle the risk is likely to occur. This risk timeframe can be a trigger during the Tracking step that alerts the team to take action if mitigation activities do not work. This timeframe should be regularly reviewed to ensure mitigation plans have been completed months before a risk could occur.

Conducting root cause analysis is also important. Since a potential risky situation consumes resources, it is beneficial to find out the root cause of a risk rather than deal with the symptoms. Root-cause analysis focuses on prevention and asking "why" questions.

2.4.3.2.3 Determine the Probability and Impact of each Risk

The third step in Qualitative Analysis is to determine the probability and impact for the risks uncovered in the Risk Identification step.

- Probability - is the likelihood that a risk will occur.
- Impact - is the consequence the risk will have on the project when it does occur.

Risks are evaluated against a standard impact/probability scale using a clearly defined range, as identified in Table 6. A clearly defined range decreases the ambiguity between different definitions of High, Moderate, and Low impact and results in a clearer picture of High priority risks. Risks with High impacts and probabilities are those that need to be addressed first.

Table 6. Risk Exposure Rating

Risk Exposure Rating	Description	Color Code
HIGH (H)	Unacceptable. Major disruption likely; different approach required; priority management attention required.	Red
MODERATE (M)	Some disruption; different approach may be required; additional management attention may be needed.	Yellow
LOW (L)	Minimum impact; minimum oversight needed to ensure risk remains low.	Green

Table 7, Risk Matrix, identifies the distribution of High (H), Moderate (M) and Low (L) Risk Exposure Rating to be used when analyzing a risk. Projects shall use this Risk Matrix or tailor it to better fit the size and scope of specific projects or management practices of the organization.

Table 7. Risk Matrix

PROBABILITY ↑	Near Certainty (0.9)	0.045	0.09	0.18	0.36	0.72
	Highly Likely (0.7)	0.035	0.07	0.14	0.28	0.56
	Likely (0.5)	0.025	0.05	0.1	0.2	0.4
	Low Likelihood (0.3)	0.015	0.03	0.06	0.12	0.24
	Not Likely (0.1)	0.005	0.01	0.02	0.04	0.08
		Marginal (0.05)	Significant (0.1)	Serious (0.2)	Very Serious (0.4)	Catastrophic (0.8)
		IMPACT →				

Examples of subjective and value assigned as ratings and the criteria for assigning Probability and Impact ratings are identified in Tables 7 and 8, below. The PM must validate these definitions or modify them as necessary for their project.

The Probability of Occurrence Rating for each root cause is established using specified criteria as shown in Table 8.

Table 8. Probability of Occurrence Rating

Rating	Value Assigned	Probability of Occurrence
Near Certainty	0.90	~90%
Highly Likely	0.70	~70%
Likely	0.50	~50%
Low Likelihood	0.30	~30%
Not Likely	0.10	~10%

Impact of each risk is divided out into cost, schedule and performance (i.e., Program and Technical - requirements/quality) consequences. The ratings and types of Impact for each risk are established using criteria described in Table 9. This Impact scale may not be appropriate for all Projects, and may need to be modified based on the situation.

Table 9. Ratings and Types of Impact Criteria

Rating	Value Assigned	Program Impact	Technical Impact	Cost Impact	Schedule Impact
Marginal	0.05	Remedy will cause program disruption	Performance goals met, no impact on program success	Program budget not dependent on issue; no impact on program success; development or production cost goals not exceeded or dependent on this issue	Schedule not dependent on this issue; no impact on program success; development schedule goals not exceeded or not dependent on the issue
Significant	0.10	Shorts a significant mission need	Performance below goal, but within acceptable limits. No changes required, acceptable alternatives exist, minor impact on program success	Program budget impacted by < 1%; minor impact on program success; development or production cost goals exceeded by 1 - 5%; program management resources do not need to be used to implement workarounds	Non-critical path activities late; workarounds would avoid impact on key and non-key program milestones; minor impact on program success, development schedule goals exceeded by 1-5%
Serious	0.20	Shorts a critical mission need	Performance below goal, moderate changes required, alternative would provide acceptable system performance, limited impact on program success	Program budget impacted by 1 - 5%; limited impact on program success; development or production cost goals exceeded by 5 - 15%; program management reserves do not need to be used to implement workarounds	Critical path activities one month late; workarounds would not meet program milestones; program success in doubt; development schedule goals exceeded by 5-10%
Very Serious	0.40	Potentially fails key performance parameter	Performance unacceptable; significant changes required; possible alternatives may exist; program success in doubt	Program budget impacted by 5-10%; program success in doubt; development or production cost goals exceeded by 15-20%; program management reserves must be used to implement workarounds	Critical path activities one month late; workarounds would not meet program milestones; program success in doubt; development schedule goals exceed by 10 -15%
Catastrophic	0.80	Jeopardizes an exit criterion of current acquisition phase	Performance unacceptable; no viable alternatives exist; program success jeopardized	Program budget impacted by 10%; program success jeopardized; development or production cost goals exceeded by 20 - 25%	Key program milestones would be late by more than 2 months; program success jeopardized; development schedule goals exceeded by 20%

Project root cause identification and analysis integrates the technical performance assessment, schedule assessment, and cost estimates using established risk evaluation techniques. Each of these risk categories (cost, schedule, and performance) has activities of primary responsibility, but is provided inputs and support from the other two risk categories. This helps to keep the process integrated and ensures the consistency of the final product.

The following paragraphs provide relevant questions to ask in assessing performance, schedule, and cost root causes.

Performance (P) Considerations

Is there an impact to performance and to what level? If so, this risk has a performance consequence. These risks generally have associated schedule and cost impacts, but should be carried as a performance risk.

- Operational
- Technical
- Management

Schedule (S) Considerations

Is there an impact to schedule performance and to what level? If the risk does not have a first order performance impact, then ask this question. If the risk impacts the critical path, then it impacts both schedule and cost, but should be carried as a schedule risk.

Were any problems that caused schedule slips identified as risks prior to their occurrence? If not, why not? If yes, why didn't the associated mitigation plan succeed?

The Team should analyze impact of the risk to the IMS and the critical path(s), to include:

- Evaluating baseline schedule inputs (durations and network logic).
- Incorporating technical assessment and schedule uncertainty inputs to the project schedule model.
- Evaluating impacts to project schedule based on technical team assessment.
- Performing schedule analysis on the project IMS, incorporating the potential impact from all contract schedules and associated government activities.
- Quantifying schedule excursions reflecting the effects of cost risks, including resource constraints.
- Providing a government schedule assessment for cost analysis and fiscal year planning, reflecting the technical foundation, activity definition, and inputs from technical and cost areas.
- Documenting the schedule basis and risk impacts for the risk assessment.
- Projecting an independent forecast of the planned completion dates for major milestones.

Cost (C) Considerations

Does the risk only impact life-cycle cost? If so, with no performance or schedule impacts, the risk is a cost risk, and may impact estimates and assessments such as:

- Building on technical and schedule assessment results;
- Translating performance and schedule risks into life-cycle cost;
- Deriving life-cycle cost estimates by integrating technical assessment and schedule risk impacts on resources;
- Establishing budgetary requirements consistent with fiscal year planning;
- Determining if the adequacy and phasing of funding supports the technical and acquisition approaches;
- Providing project lifecycle cost excursions from near-term budget execution impacts and external budget changes and constraints.
- Documenting the cost basis and risk impacts.

NOTE: Cost and Funding are not the same. **Cost** is related to the amount of money **required** to acquire and sustain a commodity. **Funding** is the amount of money **available** to acquire and sustain that commodity.

Timing Considerations

Timing is another factor that should be considered when analyzing and prioritizing risk. It can be characterized by when the Trigger Event for the risk is expected to occur. Ratings for Trigger Event Timeframes are identified in Table 9.

Table 10. Ratings for Trigger Event Date Timeframe
When Could the Trigger Event for the Risk Occur?

Rating	Trigger Event Date Timeframe
10	Immediate
9	Within the next month
8	Within the next 1 to 3 months
7	Within the next 3 to 6 months
6	Within the next 6 to 12 months
5	Within the next 12 to 18 months
4	Within the next 18 to 24 months
3	Within the next 2 to 3 years
2	Within the next 3 to 5 years
1	After 5 years

2.4.3.2.4 Calculate the Risk Exposure Score

A Risk Exposure Score is the calculation of the Impact Value (I) times the Probability Value (P) (e.g., $I * P = \text{Risk Exposure Score}$). The Risk Exposure Score is used to prioritize the long list of project risks and can be utilized for further analysis and comparisons. This calculation is completed automatically within the Risk Register.

2.4.3.2.5 Prioritize the Risks

Prioritizing a list of risks to create a Top 5 Risk List allows the PM and the team to focus resources and time on those risks that will likely cause the greatest damage to the project and negatively affect the project's objectives. The PM determines whether the team focuses on the top 3 or top 10. This decision is based on available project resources, the current state of the project and the PM's risk tolerance threshold as well as other factors.

A PM can carry this list around to discuss with stakeholders, team members and others for updates on risks and risk responses. In addition to looking at Risk Exposure scores to prioritize risks, a PM should also consider risks with lower scores, including those with a low probability but severe impact, as well as those that require an immediate response.

The list top risks should be posted in a central location where the entire team can view, validate, and respond to risks on a regular basis. Table 10 provides an example of a "Top 5 Risk List."

Table 11. Top 5 Risk List

Risk ID	Risk Description	Time Frame	Impact Rating	Probability Rating	Risk Exposure	Rank Order	Risk Owner	Risk Response
R0001	If the SE contract is not signed by 09/13, the project loses \$12 in expiring funds.	8/13	H	M	M/H	1	Name1	
R0022	If customer #5 gets approval for RFC #14 after CDR, significant design changes will be needed.	6/13	M	L	M/L	2	Name2	
R0304	If the policy on wireless technology is not signed, the alternative design #2 will be deployable, and be eliminated from design considerations	6/13	L	L	L	3	Name3	

2.4.3.2.6 Risk Register for Steps 3 & 4 Risk Analysis (Qualification & Quantification)

The process to complete Risk Analysis requires logging information into the Risk Register.

Table 11 illustrates the Risk Register Template data elements for Steps 3 & 4 Risk Analysis (Qualification & Quantification):

Table 12. Risk Register Template – Steps 3 & 4, Risk Analysis (Quantitative and Qualitative)

Risk Type (Select)	Risk Category (Select)	Risk Trigger Description (if > this)	Risk Trigger Expected Date	Potential Outcome (then > this)	Task ID	Associated Risks	Probability Rating (Select)	Prob Value	Impact Rating (Select)	Impact Value	Risk Exposure	Top 5 Y/N (Select) (See Comment)
Opportunity	Budget	If ????? occurs	Insert expected date	Then ?? Is the outcome or result	Identify Task IDs as appropriate	Identify Associated Risk as appropriate	Not Likely	0.1	Catastrophic	0.8	0.080	N

Table 12 describes the data elements entered into the Risk Register for Steps 3 and 4, Risk Analysis.

Table 13. Risk Register Data Elements for Steps 3 & 4 - Risk Analysis (Qualification & Quantification)

Cell	Definition
Risk Type	Risks can be positive (opportunity) or negative (threat.) An example of an opportunity is "The latest UML software will reduce programming efforts by 30%, thus decreasing the amount of hours needed to produce the software." An example of a threat is "A tornado can hit the remote city of Alabama as forecasted where the software developers are." Select: Threat, Opportunity, as appropriate.
Risk Category	If the risk is to occur, it will come from a root source, such as: nature, lack or abundance of technology, sponsorship, communications, schedule, budget, contracts and scope. For example, "With the support of sponsors, there will be enough resources dedicated to the project." The example references a positive risk or opportunity. Select from categories as defined by the Risk Management Plan. These values are list in cells in the Source Data Tab. Select: Technical, Sponsorship, Communication, Schedule, Budget, Contracts, Scope, as appropriate.
Risk Trigger - Description	Specifically what causes the risk to become a realized issue/problem - usually written in the form "If <"this" occurs>". Brief description of the impact (positive or negative) on the project should the Trigger event occur.
Risk Trigger - Expected Date	The estimated date on which the trigger event is expected to occur and impact the program.
Potential Outcome	What happens if the trigger event occurs - usually written in the form "then <this outcome occurs>".
Task ID	The task ID is the task defined in the network diagram, activity list or schedule that will be affected by the risk. As an example, "There is not enough feedback from end-to-end user testing when the codes are updated and changed. Members from the unit testing group will have the older codes, which will generate outdated and irrelevant applications in the future. The impact will be to the quality of the product in the next release." The unit testing tasks are the affected tasks, and their relevant Task IDs should be identified and documented in this case.
Associated Risks	Associated risks are inter-related. If an event is to take place in the near future, these other events will also take place. As an example and not a fact, "If the commercial rental rates decrease in the South where the offsite contractors are, there will be an impact on the overhead costs in the facilities of New Mexico, Arizona and Georgia" which could be associated with "the future possibility that the towns of New Mexico, Arizona and Georgia will attract less skilled and efficient employees thus harnessing the outcomes of a high-tech project."
Probability Rating	Probability of risk being realized, using scales defined in the Risk SOP. Select: Not Likely, Low Likelihood, Likely, Highly Likely, Near Certainty, as appropriate.
Probability Value	Numeric value of associated with the Probability Rating. These values are list in cells in the Source Data Tab.
Impact Rating	Qualitative ranking of impact to project, using scales defined in the Risk SOP. Select: Marginal, Significant, Serious, Very Serious, Catastrophic, as appropriate.
Impact Value	Numeric value of associated with the Impact Rating. These values are list in cells in the Source Data Tab.
Risk Exposure Score	This is calculated once you select the Impact and Probability. These cells use conditional formatting to display color shadings: Red for High, Yellow for Medium and Green for Low.

Cell	Definition
Top 5 Y/N	Top 5 Risk notation - Enter "Y" - if risk is one of the 5 top rated risks and "N" or leave blank if it rated below the top 5 risks

2.4.4 Step 5 - Risk Mitigation Planning

Risk Mitigation Planning is the process of developing options and determining actions to address the risks prioritized in the previous step. This process begins by confirming that the Risk Owners of the high-priority risks are actively focused on their assigned risks and can balance risk response planning with their other work assignments. It is the Risk Owner's job to determine what can be done to reduce the threats to project objectives and increase the project opportunities.

Risk Owners must develop:

- Risk Mitigation Strategies
- Risk Contingency Plans
- Risk Fallback Plans

Balancing the cost and schedule implications associated with risk response planning is important. Too little time dedicated to Risk Mitigation Planning could result in ineffective mitigation, contingency, or fallback plans; too much time could result in team members falling behind in other task assignments.

When planning risk mitigation responses it is important to consider when they should be executed because in many cases, timing is critical for a strategy to succeed. Consequently, it is important to look for and recognize the warning signs or risk triggers that indicate the risk condition is approaching. If any of the trigger conditions occur, the action plan for the selected mitigation strategy is implemented. Risk triggers are a way to ensure the appropriate risk mitigation strategy is implemented at the right time.

2.4.4.1 Validate Risk Owners

During Step 2, Risk Identification, team members were assigned to risks. During risk response planning, the PM should determine if the right owner is assigned to manage each risk during the project lifecycle. The Risk Owner creates the mitigation and contingency plans and is responsible for managing the risk from the analysis step through monitoring and control. They are not responsible if the risk occurs. They simply document the risk, manage the risk if it does occur, monitor the risk response effectiveness, and validate the accuracy of the risk throughout the lifecycle.

2.4.4.2 Develop Risk Mitigation Strategies

Risk Owners develop mitigation strategies for medium and high-priority risks, beginning with those on the top of the risk list. Risk Owners should complete mitigation plans within one week after the risk has been analyzed, prioritized, and added to the "Top 5 Risk List" for the project. The mitigation plan must take into consideration the estimated cost of activities and proposed schedule to implement. Mitigation plans are reviewed at the regularly scheduled risk meetings,

or other forums chosen during the Risk Management Planning (Step 1), validating the plan is cost-effective and feasible.

Mitigation plans should identify specific activities necessary to eliminate or reduce the likelihood or probability of the risk, the team members responsible for implementing the plan (if different than the Risk Owner), the triggering events that will prompt the implementation of the contingency plan, and the cost estimates for risk reserves to finance the implementation of mitigation efforts.

IMPORTANT: Add to the project schedule the activities required to implement any risk response strategies.

The Risk Owner documents the mitigation plan in the Risk Register and tracks the progress of mitigation plan activities. Triggering events for risk are monitored and reported at monthly risk review meetings.

Risk mitigation approaches are varied and require careful planning up front to mitigate or lessen the risk. Consider one or more of the following strategies:

- **Risk Avoidance:** Make changes to the project plan to eliminate the risk or to protect the project objectives from its impact by eliminating the cause. An example is a change in scope, change in technical approach, or the addition of resources to avoid or eliminate the risk.
- **Risk Transference:** Transfer responsibility and ownership of the risk to an outside resource or organization. An example is contracting out a specialized technical component when the Project Team lacks the skills.
- **Risk Acceptance:** Acknowledge the existence of the risk and accept its consequences if it occurs. An example is the acceptance of schedule or cost overrun and developing a contingency plan to execute if the risk occurs.
- **Risk Mitigation (Controlling):** Incorporate the ongoing monitoring and handling of risks throughout the life of the project to reduce the impact or probability of the risk. These mechanisms involve the use of reviews, possibly adding milestones, and development of counter measures and cost estimates. Introducing new processes or procedures to lessen the probability of producing a product that will not work or will not be accepted by users is a good example of risk mitigation.

When looking to exploit opportunities identified during the risk process the strategies include:

- **Exploitation of opportunities** - Increase the opportunity by making the cause more probable.
- **Enhancement of opportunities** - Increase the expected time savings, technical - solution, quality or cost savings by increasing the probability or impact of its occurrence
- **Acceptance of opportunities** - accept the good fortune
- **Sharing of opportunities** - keep the opportunities - don't transfer them elsewhere.

2.4.4.3 Develop Contingency Plans

Risk Owners must develop contingency plans for high-priority risks (e.g., Top 5 Risk List) and should strive to complete these within two weeks after the mitigation strategy has been identified. Contingency Plans are executed when the mitigation planning fails.

The PM using input from the team should determine if Contingency Plans are required for selected medium priority risks (e.g., those not on the Top 5 Risk List). During the weekly or monthly risk meetings, new Contingency Plans should be reviewed to validate the plans are cost-effective and feasible.

The Contingency Plan includes:

- Specific activities to be executed if the triggering event(s) occur.
- Team members responsible for implementing the plan, if different than the Risk Owner.
- Triggering events that will prompt the implementation of the Contingency Plan.
- Cost estimates for risk reserves to finance the implementation of contingency efforts.

Once Contingency Plans have been validated, the Risk Owner must ensure proper documentation is completed. Triggering events for risk must be monitored and reported at regularly scheduled project risk review meetings.

2.4.4.4 Conduct Fallback Planning

When the mitigation strategy does not work and the Contingency Plan fails, Fallback Plans are necessary to avoid derailing a project. A Fallback Plan must be created for the high-priority risks to answer the question, "If the Contingency Plan fails what should we do?" Fallback Plans must be specific to the risk, the project, and the impact on users, stakeholders and mission priorities. The Project Team must think through the details and document what needs to be done if and when the Contingency Plan fails.

For projects preparing for deployment, some of the fallback planning may be already performed and documented in the Transition Plan. Special attention must be paid to how the project affects related groups such as testers, trainers, system administrators, and end users.

2.4.4.5 Develop a Risk Response Matrix

The Risk Response Matrix is a mechanism to capture risk response strategies (e.g., avoidance, transference, acceptance, controlling), provides a concise view of the Top 5 Risk List and the corresponding responses to each risk by listing the risks on one axis and the strategies on the other. Plus and minus signs on the grid reflect positive or negative influence on other risks. This may also facilitate discussion of dependent risks and plan the risk response strategies for the project. Table 13 is a Sample Risk Response Matrix.

Table 14. Risk Response Matrix

Project Name:		Strategy #1	Strategy #2	Strategy #3	Strategy #4	Strategy #5
Top 5 Risks						
Risk Rank	Risk Description					
Risk #1						
Risk #2						
Risk #3						

Risk #4						
Risk #5						

2.4.4.6 Validate Risk Mitigation Plans and Take Action

Review each Risk Mitigation Plan to see if it is timely, realistic and the effort planned is proportionate to the severity of the risk. After the analysis of each risk response, discuss the strategies that have the greatest overall positive influence for dealing with project risks. After selecting the best approaches:

- Baseline the risk.
- Add each response to the project schedule.
- Assign resources to work on response plans.
- Regularly review progress on response plans.

2.4.4.6.1 Risk Register for Step 5 - Risk Mitigation Planning

The process to complete Step 5 - Risk Mitigation Planning requires logging information into the Risk Register.

Table 14 illustrates the Risk Register Template data elements for Step 5 - Risk Mitigation Planning.

Table 15. Risk Register Template – Step 5 – Risk Mitigation Planning

Risk Response Type (Select)	Risk Response Description
Accept	Describe planned response

Table 16. Risk Register Data Elements for Step 5 – Risk Mitigation Planning

Cell	Description
Risk Response Type	Risk responses are chosen according to their risk categories. If a risk is positive or is to bear an opportunity, the risk response type could be to accept the risk, exploit the risk or enhance the risk. If a risk is negative or it is a threat, the risk response type could be to mitigate or avoid the risk. For both situations, one can chose to transfer and share the risk with a different party. Sharing or transferring a risk can be used when the resources and expertise are limited, though many other cases lend to the option for choosing these risk responses. Select from strategies as defined by the Risk Management Plan. These values are list in cells in the Source Data Tab. Select one of the following: "Accept", "Transfer", "Mitigate/Control", "Avoid", "Share", "Exploit", and "Enhance" – as appropriate.
Risk Response Description	Based upon the choice selected for "Risk Response Type," outline how you plan on responding to the risk. An example is to "Purchase software when the company's marketing news release is made public to bring the efficiency factor up by 30%."

2.4.5 Step 6 – Risk Tracking

Risk Tracking is the process of monitoring and controlling the status and evolution of identified risks and taking appropriate measures to minimize the impact of a risk when it materializes. These measures are based on the risk mitigation or Contingency Plans developed in previous steps.

Tracking activities are determined in the risk-planning step and typically consist of the regular review of the Top 5 Risk List, triggering events, and risk timeframe dates. It is also important to validate the completeness of risk mitigation plans associated with the high-priority risks by formally conducting periodic meetings. The basic activities at this step include:

- Conducting risk review meetings to monitor risk status.
- Implementing, tracking, and updating mitigation, contingency, and fallback plans, as appropriate.
- Communicating risks and escalating when necessary.
- Formally performing risk audits.

2.4.6 Conduct Project-Level Risk Status Meetings

The format, frequency and attendee list for regular project risk status meetings are established in the Risk Management Planning step and adjusted during the project lifecycle to either increase or decrease the frequency of the meetings. The risk status meeting is the primary forum to monitor the Top 5 Risk List, including any changes to priorities, information or responses. At these meetings, the team should review:

- Top 5 Risk List for any changes (add, delete, modify).
- Triggering events and dates when the risk was projected to occur.
- Actions related to a previously unfinished risk response plans or analysis.
- Execution of risk responses to high-priority risks.
- If any corrective action is required to address a given risk.
- Issues that have arisen to determine if sufficient work is being done to solve the issue and if there are any new risks associated with this issue.
- Current state of the project to identify new risks or close other risks.

2.4.7 Validate Team-Level Attention to RM

Formal monitoring of project risk should be performed formally at status meetings and informally as a regular part of daily project activities. PMs must validate that their team leaders are following the formal RM process identified for the project during Risk Management Planning. Team Leaders and Risk Owners need to review risks they are assigned on a weekly basis to determine if:

- Documentation is clear enough that project outsiders will understand the risk.
- Information on the risk is adequate, accurate and up-to-date.
- Priority has changed.

- Risk Mitigation Plans are completed, up-to-date and accurate.
- Triggering events or expected risks timeframes are approaching.
- Mitigation, Contingency or Fallback Plans need to be executed.

2.4.8 Emphasize Risk throughout the Project Lifecycle

Risks identified by anyone on the Project Team should be documented, discussed and recorded in the Risk Register. After Mitigation/Contingency Plans have been developed, careful monitoring of risks is required to minimize the impact if a risk materializes. Any issues that have arisen should be proactively addressed and the team should consider whether any related issue may have been missed. Often there are ripple effects when a risk occurs.

2.4.9 Communicate Risks

The more visibility given to the risk, the less likely it is to occur because so many people are focused on it; therefore, find ways to keep communication open among the Project Team, management team, stakeholders, and other entities that could help mitigate or eliminate the risk.

Consider the following to highlight the Project risks:

- Post the Top 5 Risk List in team gathering places or formal war rooms.
- Include the Risk Response Matrix describing the Top 5 Risk List in regular status reports, Executive Dashboards and distribute to each of the stakeholders associated with your Project.
- Include the Top 5 Risk List, risk responses, and resource needs in Monthly Project Reviews.
- Highlight in color on a network diagram those project activities that have the highest risk.
- Before every control gate or milestone, discuss the current list of risks and solicit new solutions to mitigate or eliminate risks and to identify any new risks.

2.4.10 Escalate Risks

There may be risks requiring attention at higher levels within the Agency, especially those with potential impact across projects or an adverse impact to IT investments. For example, some risks may require Risk Mitigation Plans more costly or time-consuming than feasible for a given project.

2.4.11 Initiate More Oversight for Tasks with High Risk

For each task that includes a high-priority risk, consider using formal documentation to obtain timely information about the task. As input into weekly status and/or risk meetings, ask the team member responsible for a task to document any changes to schedule, scope, or cost; current status; problems or issues; and any risks. Ask them to bring a signed hard copy to the status meeting to be used for discussion.

2.4.12 Conduct Risk Audits

A risk audit is conducted to examine the effectiveness of the risk process, mitigation strategies, Contingency and Fallback Plans. The auditor, who can be a member of the Project Team or an independent party, also makes a determination if the correct Risk Owners are assigned to the risks.

On large complex projects, a risk audit should be done before the Risk Management Plan is approved. However, a risk audit is generally done during project execution and produces recommendations in a formal report. Such recommendations may include reassigning Risk Owners and/or updating the Mitigation Strategies, Contingency and Fallback Plans.

2.4.12.1 Risk Register for Step 6 - Risk Tracking

The process to complete Step 6 - Risk Tracking - requires logging information into the Risk Register.

Table 17 illustrates the Risk Register Template data elements for Step 6 - Risk Tracking

Table 17. Risk Register Template – Step 6 – Risk Tracking

Risk Trigger Occurrence (Select)	Trigger Date Occurrence	Status (Select)	Notes
N	Insert date Trigger occurred	Identified	Add notes as appropriate

Table 18. Risk Register Data Elements for Steps 6 – Risk Tracking

Cell	Definition
Risk Trigger Occurrence	The risk trigger occurrence communicates if the risk has or has not taken place. Select "YES" or "NO"
Trigger Date Occurrence	If triggered, the date the trigger occurred. The risk trigger occurrence communicates if the risk has or has not taken place.
Status	Risk status (e.g. whether it has been triggered or not). Select from one of the values listed in the drop down list. Select: Identified, Analysis, Complete, Planning Complete, Triggered, Resolved, Retired, Cancelled, as appropriate.
Notes	Additional notes - use as required to expand on explanations or provide reminders.

3. Appendix A: Acronym List

Table 19. Acronym List

Acronym	Definition
BSME	Business Subject Matter Expert
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
CONOPS	Concept of Operations
EVM	Earned Value Management
GOTS	Government Off-the-Shelf
IBC	Investment Business Case
IMS	Integrated Master Schedule
ISDDG	Information Services Design and Development Group
IS	Information Services
IT	Information Technology
LCC	Lifecycle cost
OMB	Office of Management and Budget
NIST	National Institute of Standards and Technology
PM	Project Manager
PMO	Project Management Office
PMP	Project Management Plan
RBS	Risk Breakdown Structure
RM	Risk Management
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SWOT	Strengths, Weaknesses, Opportunities, Threats
WBS	Work Breakdown Structure
XLC	Expedited Life Cycle

4. Appendix B: Risk Identification (Step 2) Techniques Descriptions

1. Brainstorming

Invite each member of the Project Team and key stakeholders to a risk identification session with the objective of generating a list of risks for the project. Multiple brainstorming sessions with different groups of people may be needed with larger teams. Ask those in attendance to identify the risks related to the project as a whole. Then ask questions related to the major tasks on your project schedule. If time allows, ask for risks by category (e.g., technical, schedule, resources, financial, external, etc.).

Discuss the topics, risks, issues and problems that arise and use a scribe to capture the information discussed, so it can be evaluated in more detail at a later date. Do not evaluate the ideas during the session, but simply try to capture the information in cause-risk-effect format (See Section 1.3 Risk Definition). Once all the risks have been identified, the team can discuss each risk to determine its relevance and priority.

Structured Reviews of Project Documentation

Choose a key project deliverable associated with the current phase of the project (e.g., the Requirements Document in the “Initiation, Concept and Planning” Phase), then discuss it section by section with a representative sample of project stakeholders to uncover events or circumstances that could derail the project. Another structured way to uncover risks is to compare documents (e.g., the requirements document vs. the WBS) to identify gaps and risks that can result from those gaps.

Look at internal and external risks by examining documentation, historical information, project dependencies and changing situations to uncover circumstances or potential events that may impact the ability of the project to meet its objectives.

Internal project documentation may include:

- IBC - examine the benefits and risks listed and the measures of success
- Project Management Plan (PMP) - review each section for completeness and areas of uncertainty
- Project Charter - determine if all stakeholders have signed; later in the lifecycle compare charter to current state of the project to determine if the solution is based on the original business need
- Staffing Plan - review monthly to review open positions, anticipated new positions, and succession planning
- Scope Statement - evaluate the completeness of this statement and the project management processes developed to keep the project within scope
- Schedule - evaluate the task duration and resources, dependencies, and milestone dates for reasonableness
- Requirements Document - review for gaps compared to the customer Concept of Operations (CONOPS) and for vague or unclear requirements

- Cost Estimates - evaluate the reasonableness of cost estimates compared to the WBS and schedule
- Technical Specifications - evaluate level of detail and thoroughness
- Interface Control Documents - determine if all interfaces have been defined; evaluate if the team has sufficient technical knowledge of the interface(s)
- Contract - evaluate contract type, incentives, and disincentives to identify where the government needs to focus oversight/risk management efforts
- Assumption and Constraint Lists - review current and previous documentation related to projects using the same technology, customer base, and infrastructure
- Historical Information - search for and review old project documentation; consider PM's or other team members' previous experience on this project (or similar projects).

External project dependencies are often overlooked and can easily derail a project if ignored:

- End-user expectations, priorities, and schedules
- Schedules of projects on which your project is dependent
- Funding
- Policies
- Stakeholders of projects on which your project is dependent

2. Sticky Notes

Invite to a risk identification session each member of the Project Team and key stakeholders who clearly understand the project scope and major issues associated with achieving project objectives. Give everyone a pad of sticky notes (Post-it™ Notes) and ask them to write down the first 5 to 10 roadblocks to project (i.e., one risk/roadblock per sticky note.). When finished, ask them to post the notes to the white board. Alternatively, the PM can pose a question (e.g., what could go wrong when deploying the system to Central America) and have each person write down different risks on their notes. Once finished, organize the notes by category and see if other risks are generated by examining the categorized risks.

Another variation on the sticky-note technique is to post a large network diagram of the schedule on the wall and have participants in this exercise place sticky notes on the risks related to the tasks: dependencies, durations, and other schedule elements.

3. Affinity Diagrams

Leveraging the work done in the sticky-note exercise, ask the group who identified the risks to categorize them by placing risks that are similar into columns. Participants need to negotiate and make decisions on where to place the risks by using hand and eye gestures rather than by talking to each other. After the group has finished, talking can resume and column titles can be suggested for each set of risks.

4. Checklists

Checklists provide specific areas where the team can begin to brainstorm and identify project risks. (Appendix D contains a list of possible risk categories.) The following list is taken from a large Agency program with a proven RM process and takes into consideration both internal and external project risks:

- Technical, quality, and performance

- Financial
- Schedule
- Programmatic
- Interdependencies
- Competing interests
- Legal/Contracting
- Unpredictable (e.g. hurricanes, snowstorms, regulatory)
- Predictable, but uncertain events (e.g., volatile world events)
- Organizational
- Supportability
- Stakeholder commitment and satisfaction
- Vendors and suppliers
- Culture

CAUTION: Some RM experts believe checklists should be used at the end of the identification phase to validate that key areas or categories of risk have not been overlooked. It is important not to use this list of categories at the start of risk identification, because the goal is to get participants to capture unbiased, original thought. Many checklists or structured lists are generic and others cater to Information Services (IS) projects, but they are not tailored to the unique characteristics of the project. This may limit the identification process if people are only focused on the topics in the checklist and not on those risks specific to the project.

5. Risk Breakdown Structure (RBS)

This technique is typically used to identify showstoppers to project success. A list of standard risk categories and causes in the form of a checklist is a great memory jogger that can generate discussion and help people identify the breadth of risks in certain areas.

Using this technique may limit the number and variety of risks identified, but if this approach is used in conjunction with another approach aimed at capturing risks at the task level, this technique is helpful in capturing the big events that have a major effect on the project.

RM specialists created a set of universal project risks, which have evolved into a way to organize risks using a RBS. An RBS is a source-oriented grouping of project risks that organizes and defines the total risk exposure of the project. Each descending level represents an increasingly detailed definition of sources of risk to the project. Figure 2 provides an example.

Figure 2. Risk Breakdown Structure - Example

Level 0	Level 1	Level 2	Level 3
Project Risks	Technical	Hardware Platform	Capacity
			Reliability
		Development Environment	Process Control
			Tools
	Programmatic	Scope Management	Scope Definition
			Change Management Process
		Requirements	Stability
			Completeness
		Contractual	Incentives/Disincentives
	Stakeholder	Sponsor	Clarity of Vision
			Involvement
		Customer	Clear Understanding and Knowledge
			Involvement
		OIS/OAGM	Involvement
			Understanding of Solution
	Team	CIO	Investment Priority
		Involvement	
Technical Resources		Staffing Plan	
		Outsourcing	
	Subject Matter Resources	Availability	
		Cost	

Assumptions analysis is typically done at the beginning of a project, when there is a change to the project environment or when major decisions have been made. Your project documentation includes assumptions and constraints related to the technical environment, staffing levels, project dependencies and other related factors that can be analyzed to identify some project risks.

There are assumptions related to every risk identified. For example, the following risk, "During the design stage, if an additional five system engineers with skills in J2EE are not available, then design documentation will not be delivered on time in accordance with the baseline schedule," assumes that five engineers have the engineering and documentation skills to do the work within the time allotted. A different assumption would be to use three engineers and two technical writers.

It is important that assumptions are adequately identified before proceeding to risk analysis. Ask the questions:

- What assumptions have been made?
- Are these assumptions correct?
- Are the assumptions realistic?

PMs can also list the project deliverables stating some known facts about them. Ask end users, stakeholders and the Project Team what their perspective is on a project deliverable (e.g., GUI, training plan, schedule) or if they agree with the assumptions. For example, is there clarity on access control? Should access control be at the folder level, the document level, and/or within portions of the document? Do stakeholders think that end-user training is Web-based, but the team is planning to have help features embedded in the application?

6. Taxonomy-Based Risk Identification

The Software Engineering Institute/Carnegie Mellon University developed a Taxonomy-based Risk Identification method that organizes software development risks in a manner to provide structured brainstorming. The method uses a taxonomy of software development risks that provides a framework for organizing and understanding software development issues. This framework provides a structured way to expose risks that impact software development projects.

The method includes a standard process and a taxonomy-based questionnaire. The taxonomy organizes risks into three levels—class, element, and attribute. The questionnaire has questions under each attribute designed to elicit risks and issues potentially affecting the project.

7. Expert Interviews

Identify a list of people who have the expert knowledge to understand your project requirements, implementation issues, and concept of the final solution. Spend considerable time preparing for the interview questions so during the interview you'll capture the information needed to make your project a success. Fully understand what you want to gain out of each interview and think about the questions you want to ask.

At the interview, before asking the prepared questions, explain your objectives and introduce the note taker or scribe. Ask open-ended questions related to the project methodology and proposed solution to get some perspective on the person you are interviewing before going through the list of questions.

As you ask your questions, evaluate the responses. If they are vague, ask more pointed questions to drill down to the specific information needed. When responses are not fully understood, ask for clarification. As you finish the interview, document your interview session and send your notes to the expert for validation.

8. Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis

SWOT Analysis focuses on identifying risks from the organizational perspective rather than just within the boundaries of the Project Team. This technique is designed to examine the organization in four ways:

<u>Strengths:</u>	What is done well by the organization and/or Project Team?
<u>Weaknesses:</u>	What deficiencies do we have as an organization or Project Team?
<u>Opportunities:</u>	What external forces may work in the project's favor and how can the team take advantage of it?
<u>Threats:</u>	What external forces may work against the team and how can they be mitigated?

This technique is typically performed early in the project to understand the risk environment and to communicate to management the factors impacting the project. Results from this analysis allow the PM to present the pros and cons of the project openly. Furthermore the results can be used to encourage management to alter some environmental factors to positively impact the project's performance.

This method will not help PMs uncover detailed project risks. However, it will provide a way for PMs to document the state of the project environment at the start of the project so that if problems do occur, the PM can be assured that management was informed about them early.

9. Lessons Learned

At the end of each project phase (and at the end of the project itself), the team should discuss what was learned during the project or previous phase, and an evaluation of the project risk should be done. A Lessons Learned discussion considers all aspects of a project—resources, schedule, budget, and scope—and asks the following questions:

- What went well and what went wrong?
- What could have been done differently to improve the project?
- What conditions existed that helped or hindered the project to achieve its objectives?

Specifically for RM, the lessons learned should include an evaluation of how the risk effort was handled and how it can be improved next time.

Capturing lessons learned could help the next PM who is responsible for the project. The team developing the system may be different from the team operating and maintaining the system, but many of the on-going issues or potential risks may remain the same.

Lessons Learned can be captured or applied at specific points in the standard lifecycle. For example, the testing function can provide a strong focus on risk because of their specific role. They can identify risks that may arise if the application moves forward based on their knowledge of the environment and the specific functionality that did not pass the test scenarios.

10. Delphi Technique

This survey technique is used when there are only a handful of experts who can provide the required insight into the project. It is a time-consuming but proven technique that allows the Project Team to obtain insights from professionals who otherwise would not contribute to the success of the project.

It requires a Delphi facilitator to develop and present the questions in a manner that will get results. The questions need to address the risk areas of concern and prompt the recipients to provide information that will be valuable to the project.

Steps:

- 1) Identify those who have a stake in the project.
- 2) Create a list of questions to draw out information of value.
- 3) Ask for responses to the questions. Email can be used to distribute the list of questions where responses are captured electronically or an interview is scheduled to collect the information. Alternatively, a group of designated experts can be invited to a meeting where they complete the questionnaire individually.
- 4) Review and restate the responses to identify common topics, issues, and concerns; then return the information to the participants for validation.
- 5) Gather opinions and repeat as often as necessary to fully understand project risks.
- 6) Document the results explaining how and where the information obtained will be used.

5. Appendix C: Risk Register Template

SUMMARY: **AUTO POPULATED - DO NOT ENTER DATA HERE**

Project Name XLC Steering Committee - Risk Register Demo
 Project Manager Insert Project Manager Name(s)
 Funding No. Insert Funding No.
 Technology Deployed: 0

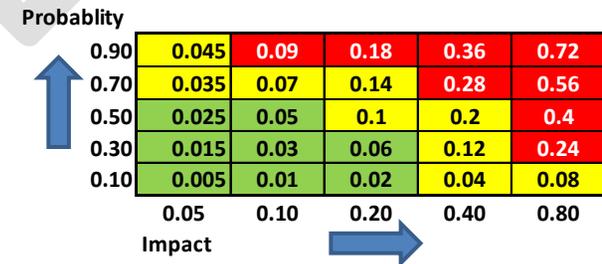
TO BE DEVELOPED

SUMMARY - RISK COUNT BY RATING	
Rating	#
HIGH (H) (Red)	0
MODERATE (M) (Yellow)	0
LOW (L) (Green)	0
TOTAL	0

TO BE DEVELOPED

TOP 5 RISKS			
Risk #	Risk ID	Risk Title	RiskExposure
Risk 1			
Risk 2			
Risk 3			
Risk 4			
Risk 5			

Risk Matrix



HIGH (H) – Unacceptable. Major disruption likely; different approach required; priority management attention required.

MODERATE (M) – Some disruption; different approach may be required; additional management attention may be needed.

LOW (L) – Minimum impact; minimum oversight needed to ensure risk remains low.

LEGEND:		
Administrative	Project Name	Enter the official Title/Name of the Project
	Project Manager	Individual responsible for creating, updating and maintaining the integrity of the risk register. Individual assigned with the responsibility of documenting risks and orchestrating project risk updates with the risk owners.
	Funding No.	The funding number is assigned by the OFM (Office of Financial Management) once the project is approved for funding.
	Technology Deployed	Technology deployed is the category or component of a system under development in this project. The categories of technologies currently available are: Mid-tier (application), Desktop, Mainframe, Database, Infrastructure, Office Automation or Telecommunications.
Risk Identification	Risk ID	A unique identifier in a numbering system assigned to a risk. The identifier should be used for reference or for cross-reference in the future among project team members and future project stakeholders in search of historical information. Example: R01, R02, R03...
	Date Identified	The original date when the risk was originally brought to light, or identified. Example: "MMDD/YY"
	Risk Submitter	The name of the individual or group who identified and submitted the risk to bring the attention of project stakeholders.
	Risk Title (NEW)	Short title/description of the risk - No more than 10 words
	Risk Description	A brief description of future event that could result in either positive or negative results to the project, and the impact it will have on the project.
	Source (NEW)	Source of risk. These values are list in cells in the Source Data Tab.
	Risk Owner	The risk owner is the individual assigned to the project who tracks the risks for triggers.
	Risk Type	Risks can be positive (opportunity) or negative (threat.) An example of an opportunity is "The latest UML software will reduce programming efforts by 30%, thus decreasing the amount of hours needed to produce the software." An example of a threat is "A tornado can hit the remote city of Alabama as forecasted where the software developers are." Select "Threat" or "Opportunity" as appropriate
	Risk Category	If the risk is to occur, it will come from a root source. such as: nature, lack or abundance of technology, sponsorship, communications, schedule, budget, contracts and scope. For example, "With the support of sponsors, there will be enough resources dedicated to the project." The example references a positive risk or opportunity. Select from categories as defined by the Risk Management Plan. These values are list in cells in the Source Data Tab.
	Risk Trigger - Description	Specifically what causes the risk to become a realized issue/problem - usually written in the form "If <"this" occurs>". Brief description impact (positive or negative) on the project should the risk event occur.
	Risk Trigger- Expected Date (NEW)	The estimated date on which the trigger event is expected to occur and impact the program.
	Potential Outcome (MODIFIED)	What happens if the trigger event occurs - usually written in the form "then <this outcome occurs>".
	Task ID	The task ID is the task defined in the network diagram, activity list or schedule that will be affected by the risk. As an example, "There is not enough feedback from end-to-end user testing when the codes are updated and changed. Members from the unit testing group will have the older codes, which will generate outdated and irrelevant applications in the future. The impact will be to the quality of the product in the next release." The unit testing tasks are the affected tasks, and their relevant Task IDs should be identified and documented in this case.
	Associated Risks	Associated risks are inter-related. If an event is to take place in the near future, these other events will also take place. As an example and not a fact, "If the commercial rental rates decrease in the South where the offsite contractors are, there will be an impact on the overhead costs in the facilities of New Mexico, Arizona and Georgia" which could be associated with "the future possibility that the towns of New Mexico, Arizona and Georgia will attract less skilled and efficient employees thus harnessing the outcomes of a high-tech project."
Risk Analysis	Probability Rating	Probability of risk being realized, using scales defined in the Risk Management Plan. (See Prob-Impact Matrix tab)
	Prob Value (NEW)	Numeric value of associated with the Probability Rating. These values are list in cells in the Source Data Tab.
	Impact Rating	Qualitative ranking of impact to project, using scales defined in the Risk Management Plan. (See Prob-Impact Matrix tab)
	Impact Value (NEW)	Numeric value of associated with the Impact Rating. These values are list in cells in the Source Data Tab.
	Risk Exposure Score (MODIFIED)	This is calculated once you select the Impact and Probability. These cells use conditional formatting to display color shadings as defined in the Source Data Tab. . (For explanation of Impact and Probability - See Prob-Impact Matrix tab)
Risk Mitigation Planning	Top 5 Y/N (NEW)	Top 5 Risk notation - Enter "Y" - if risk is one of the 5 top rated risks and "N" or leave blank if it rated below the top 5 risks
	Risk Response Type	Risk responses are chosen according to their risk categories. If a risk is positive or is to bear an opportunity, the risk response type could be to accept the risk, exploit the risk or enhance the risk. If a risk is negative or it is a threat, the risk response type could be to mitigate or avoid the risk. For both situations, one can chose to transfer and share the risk with a different party. Sharing or transferring a risk can be used when the resources and expertise are limited, though many other cases lend to the option for choosing these risk responses. Select from strategies as defined by the Risk Management Plan. These values are list in cells in the Source Data Tab. Select one of the following: "Accept", "Transfer", "Mitigate", "Avoid", "Share", "Exploit", "Enhance" - .
Risk Monitoring & Control	Risk Response Description	Based upon the choice selected for "Risk Response Type," outline how you plan on responding to the risk. An example is to "Purchase software when the company's marketing news release is made public to bring the efficiency factor up by 30%."
	Risk Trigger Occurance	The risk trigger occurrence communicates if the risk has or has not taken place. Select "YES" or "NO"
	Trigger Date Occurance (NEW)	If triggered, the date the trigger occurred. The risk trigger occurrence communicates if the risk has or has not taken place.
	Status	Risk status (e.g. whether it has been triggered or not). Select from one of the values listed in the drop down list. These values are list in cells in the Source Data Tab.
	Notes (NEW)	Additional notes - use as required to expand on explanations or provide reminders.

Project Name:		XLC Steering Committee - Risk Register Demo							Project Manager	Insert Project Manager Name(s)	Funding No.	Insert Funding No.				Technology Deployed:										
Risk Identification														Risk Analysis					Risk Mitigation Planning				Risk Tracking			
Risk ID	Date Identified	Risk Submitter	Risk Title	Risk Description	Source (Select)	Risk Owner	Risk Type (Select)	Risk Category (Select)	Risk Trigger Description (If > this)	Risk Trigger Expected Date	Potential Outcome (then > this)	Task ID	Associated Risks	Probability Rating (Select)	Prob Value	Impact Rating (Select)	Impact Value	Risk Exposure	Top 5 Y/N (Select) (See Comments)	Risk Response Type (Select)	Risk Response Description	Risk Trigger Occurrence (Select)	Trigger Date Occurrence	Status (Select)	Notes	
R001	4-Apr-13	Insert Name	Insert short title	Insert description	Stakeholder	Insert Name	Opportunity	Budget	If ????	Insert expected date	Then ?? Is the outcome or result	Identify Task IDs as appropriate	Identify Associated Risk as appropriate	Not Likely	0.1	Catastrophic	0.8	0.080	N	Accept	Describe planned response	N	Insert date Trigger occurred	Identified	Add notes as appropriate	
R002	5-Apr-13	Insert Name	Insert short title	Insert description	Stakeholder	Insert Name	Threat	Schedule	If ????	Insert expected date	Then ?? Is the outcome or result	Identify Task IDs as appropriate	Identify Associated Risk as appropriate	Near Certainty	0.9	Significant	0.1	0.090	Y	Mitigate	Describe planned response	Y	Insert date Trigger occurred	Planning Complete	Add notes as appropriate	
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A								
														#N/A		#N/A	#N/A	#N/A</								

Risk Exposure Score Calculation

Impact Ratings

Rating	Value Assigned	Program Impact	Technical Impact	Cost Impact	Schedule Impact
Marginal	0.05	Remedy will cause program disruption	Performance goals met, no impact on program success	Program budget not dependant on issue; no impact on program success; development or production cost goals not exceeded or dependant on this issue	Schedule not dependant on this issue; no impact on program success; development schedule goals not exceeded or not dependant on the issue
Significant	0.10	Shorts a significant mission need	Performance below goal, but within acceptable limites. No charnges required, acceptable alternatives exist, minor impact on program success	Program budget impacted by < 1%; minor ipact on program success; development or production cost goals exceeded by 1 - 5%; program management reserces do not need to be used to implement workarounds	Non-critical path activities late; workarounds would avoid impact onkey and non-key program milestones; minor impact on program success, development schedule goals exceeded by 1-5%
Serious	0.20	Shorts a critital mission need	Performance below goal, moderate changes required, alternative would provide acceptable system performance, limited impact on program success	Program budget impacted by 1 - 5%; limited impact on program success; development or production gost goals exceeded by 5 - 15%; program managemnet reserves do not need to be used to implement workarounds	Critical path activiites onemonth late; workarounds would not meet program milstones; program success in doubt; development schedule goals exceeded by 5 10%
Very Serious	0.40	Potentially fails key performance parameter	Performance unacceptable; signigicant changes required; possible alternaitves may exist; program success in doubt	Program budget impacted by 5-10%; program success in doubt; development or production cost goals exceeded by 15- 20%; program management reserves must be used to implement work arounds	Critical path activities one month late; workarounds would not meet program meilestones; program success in doubt; development schedule goals exceed by 10 -15%
Catastrophic	0.80	Jeoporadizes an exit criterion of current acquisition phase	Permanace unacceptable; no viable alternatives exist; program success jeopardized	Program budget impacted by 10%; program success jeoporadized; development or production cost goals exceeded by 20 - 25%	Key program milestones would be late by more than 2 months; program success jeoporadized; development schedule goals exceeded by 20%

Probablity Ratings

Rating	Value Assigned	~10%	~30%	~50%	~70%	~90%
Not Likely	0.10					
Low Likelihood	0.30					
Likely	0.50					
Highly Likely	0.70					
Near Certainty	0.90					

Risk Impact Calculation: Sum of: (Impact Value) * (Probability Value) ----- (LINKED)

Probability	0.90	0.70	0.50	0.30	0.10
0.90	0.045	0.090	0.180	0.360	0.720
0.70	0.035	0.070	0.140	0.280	0.560
0.50	0.025	0.050	0.100	0.200	0.400
0.30	0.015	0.030	0.060	0.120	0.240
0.10	0.005	0.010	0.020	0.040	0.080
Impact	0.05	0.10	0.20	0.40	0.80

TECHNOLOGY DEPLOYED
Mid-Tier (Application)
Desktop
Mainframe
Database
Infrastructure
Office Automation
Telecommunications

Risk Source
Formal Risk Review
Audit/Review
Status Meeting
Stakeholder
Other

Risk Type
Threat
Opportunity

Risk Category
Technical
Sponsorship
Communication
Schedule
Budget
Contracts
Scope

LINKED

Impact Rating	
Marginal	0.05
Significant	0.10
Serious	0.20
Very Serious	0.40
Catastrophic	0.80

LINKED

Probability Rating	
Not Likely	0.10
Low Likelihood	0.30
Likely	0.50
Highly Likely	0.70
Near Certainty	0.90

Risk Response Type
Accept
Transfer
Mitigate/Control
Avoid
Share
Exploit
Enhance

Risk Trigger Occurance
Y
N

Status
Identified
Analysis Complete
Planning Complete
Triggered
Resolved
Retired
Cancelled

DO NOT REMOVE LINKED TO TOOL

Green/Yellow/Red Threshold Values	
Green - maximum score	0.05
Yellow - minimum score	0.06
Yellow - maximum score	0.14
Red - minimum score	0.15
White - Blank Cell	0.00

Y/N
Y
N

TO BE DEVELOPED

Risk Count by Threshold Value	
High	
Medium	
Low	
Total	

Acronyms

Table 20. List of Acronyms

Acronym	Literal Translation
BSME	Business Subject Matter Expert
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
CONOPS	Concept of Operations
EVM	Earned Value Management
GOTS	Government Off-the-Shelf
IBC	Investment Business Case
IMS	Integrated Master Schedule
ISDDG	Information Services Design and Development Group
IS	Information Services
IT	Information Technology
LCC	Lifecycle cost
OMB	Office of Management and Budget
NIST	National Institute of Standards and Technology
PM	Project Manager
PMO	Project Management Office
PMP	Project Management Plan
RBS	Risk Breakdown Structure
RM	Risk Management
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SWOT	Strengths, Weaknesses, Opportunities, Threats
WBS	Work Breakdown Structure
XLC	Expedited Life Cycle

Glossary

Table 21. Glossary

Term	Definition
Business Requirement (BR)	A BR is a statement of the functions needed in order to accomplish the business objectives. It is the highest level of requirement, developed through the dictation of policy and process by the business owner.
Business Rule (RU)	An RU is a statement that defines or constrains some aspect of the business. It is intended to assert business structure, or to control or influence the behavior of the business. The RUs that concern the project are atomic in that they cannot be further decomposed and they are not process-dependent, so that they apply at all times. Business rules typically fall into one of five categories: terms, facts, derivations, assertions or action enablers.
Functional Requirement (FR)	An FR is a statement of an action or expectation of what the system will take or do. It is measured by concrete means like data values, decision making logic and algorithms.
Nonfunctional Requirement (NR)	An NR is a low-level requirement that focuses on the specific characteristics that must be addressed in order to be acceptable as an end product. NRs have a focus on messaging, security, and system interaction.
Scenario	A scenario is a sequence of steps taken to complete a user requirement, similar to a use case.
Use Case	A use case is a description of a system's behavior as it responds to a request that originates from outside of that system. The use case is made up of a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal. The use case should contain all system activities that have significance to the users. Use cases typically avoid technical jargon, preferring instead the language of the subject matter expert.
User Requirement (UR)	A UR is a statement of what users need to accomplish. It is a mid-level requirement describing specific operations for a user (e.g., a business user, system administrator, or the system itself). They are usually written in the user's language and define what the user expects from the end product.

Related Documents

Table 22. Related Documents

Document Name	Document Number and/or URL	Issuance Date
XLC Process Overview	https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html	
Risk Management Handbook Volume I Chapter 10, CMS Risk Management Terms, Definitions, and Acronyms, FINAL Version 1.0	https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VI_10_Terms_Defs_Acronyms.pdf	July 13, 2012
Risk Management Handbook Volume I Chapter 1, Risk Management in the XLC	https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/InformationSecurity-Library-Items/RMH-Vol-I-Chapter-01-Risk-Management-in-the-XLC.html	November 8, 2012
Risk Management Plan Template	https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/RiskMgmtPlan.docx	
Risk Register Template	https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/RiskRegister.xlsx	

Template Revision History

Table 23. Revision History

Version Number	Revisions Made	Date of Revisions	Author
0.1	SOP-Draft	5/10/2013	Tom Hydock (Noblis)
0.2	Reduced content at clients request	5/20/2013	Tom Hydock (Noblis)
1.0	Content revised to be consistent with Risk Management Plan included in the CMS Expedited Life Cycle (XLC)	6/19/2013	Tom Hydock (Noblis)
2.0	Removed Risk Management Plan and reformatted document with XLC template.	5/30/2014	Celia Shaunessy (CMS/OIS/EASG/DITG)

Approvals

The undersigned acknowledge that they have reviewed this document and agree with the information presented within it. Changes to this document will be coordinated with, and approved by, the undersigned, or their designated representatives.

Signature: _____ Date: _____

Print Name: XLC Steering Committee

Title: _____

Role: CMS' Approving Authority
