Risk Management Procedure
OETI-PMP-05

Environmental Protection Agency
Office of Enterprise Technology and Innovation (OETI)

February 23, 2007 – Version 1.0

Document Change History

Version	Date	Author	Description of Changes

Contents

1. Introduction 1
1.1 Purpose 1
1.2 Background 1
2. Approach 2
2.1 Assumptions 2
2.2 Scalability 2
2.3 Best Practices 3
3. Roles and Responsibilities 5
4. Procedure 7
4.1 Process Flow Diagram 7
4.2 Steps 7
4.2.1 Risk Planning 8
4.2.2 Identify Risks 9
4.2.3 Analyze Risks 12
4.2.4 Plan Risk Responses 16
4.2.5 Escalate Risk or Risk Response 18
4.2.6 Implement Risk Response Plan 18
4.2.7 Control and Monitor Risks 19
4.2.8 Close Risks 20
5. Considerations 21
Appendix A. Acronyms A-1
Appendix B. Checklist B-1
Appendix C. Additional Resources C-1
Appendix D. Interface Requirements D-1
Appendix E. Risk Management Plan Template E-1
Appendix F. Risk Reporting Form F-1
Appendix G. Risk Category Alignment with OMB Exhibit 300 ..... G-1
Appendix H. Risk Log H-1

Appendix I. Risk Management Report I-1

1. Introduction

This document defines the process by which staff within the Environmental Protection Agency (EPA)'s Office of Enterprise Technology and Innovation (OETI) performs risk management activities.

1.1 Purpose

This document defines the approach, process flow, and relevant standards by which OETI project staff performs risk management activities and identifies participants and their responsibilities.

1.2 Background

Risk management is a systematic, iterative process of identifying, analyzing, and responding to risks to the achievement of project objectives. Continuous risk management (CRM) is a forward-looking process that provides management with the capability to be proactive rather than reactive in managing potential impacts to the project. The objective of CRM is to implement risk management practices during the project to enable informed decision making, optimization of resources, and prevent cost, schedule, and technical performance risks from becoming issues that can adversely impact the project. A CRM approach is therefore applied to anticipate and mitigate the risks that could have a critical impact on project performance. Project risk management is defined as "increasing the probability and impact of positive events, and decreasing the probability and impact of events adverse to the project."[1]

Risks are defined as having two basic characteristics: "1) Uncertainty – The risk may or may not occur and 2) Loss – The event has unwanted consequences or losses."[2] Risks differ from issues in the uncertainty characteristic. Issues have occurred; risks may or may not. To address the unique characteristics of risks, CRM assesses what could potentially go wrong and have negative consequences for the project. The process requires careful consideration of which potential events are important enough to address. For large, complex projects, a Risk Management Committee may be established to formalize and facilitate the CRM process. A Risk Management Committee is typically made up of key stakeholders, and key members of the project team. The Risk Management Committee meets on a regular basis to analyze, prioritize and manage project risks.

---

[1] Project Management Institute, The Project Management Body of Knowledge *(PMBOK®)*, Third Edition. 2004 Appendix B, Section B.3, p 252.

[2] NASA, "Continuous Risk Management at NASA" presented at the Applied Software Measurement/Software Management Conference, February 1999, San Jose, CA.

2. Approach

This section explains the approach used to develop this risk management procedure. It details the assumptions, the degree of scalability of this procedure, and the industry standards, best practices, and EPA current practices consulted in creating this procedure.

2.1 Assumptions

The following assumptions guide this risk management procedure:

- CRM applies to activities as performed by both EPA and contractors supporting OETI projects.
- The Risk Coordinator will maintain documents using the document management procedures and tools defined for the project. (See *PMP-12 Document Management Procedure*.)
- A risk tracking tool or spreadsheet will be used to capture and track risks over the life of the project.
- For system projects, the Office of Environmental Information (OEI) System Life Cycle Management (SLCM) policy and procedures apply.
- The Risk Management Plan is a living document and its users continually update it over the life cycle of the project as new requirements, change requests, re-planning activities, and external events occur.

2.2 Scalability

The Project Manager determines to what extent to implement risk management as well as the details of the process during project planning. The timing of project planning activities is discussed in *PMP-02 Project Initiation and Planning Procedure*. Because CRM provides decision makers with important information for administering projects, the risk management procedure applies for all projects initiated by OETI. However, this procedure can be scaled relative to the type of project, project size, cost, duration, control over resources, use of new technology, number of stakeholders, potential business impact of the project, extent of dependencies on other teams or events, and complexity rating for the project. For more information on assignment of complexity rating for the project, refer to PMP-02. Table 2-1 below provides basic guidelines for determining the extent to which this risk management procedure is implemented for a given project.

Table 2.1. Risk Management Procedure Scalability Guidelines

Procedure	Does the Procedure Apply?	Determining Procedure Scalability
OETI-PMP-05 Risk Management Procedure	Applies to all projects	▪ Procedure is scaled based on project size, cost, duration, control over resources, use of new technology, number of stakeholders, and the potential business impact of the project ▪ Development of a project risk management plan is required for system projects ▪ Large, complex, or unique projects tend to face a greater number of risks and require more rigor in managing risks

The risk management process can be informal or formal, depending on the size, scope, and complexity of the project. This procedure addresses the risk management process for large, complex projects. Smaller and more routine projects may implement a subset of these steps or scaled-down versions of the risk management activities. Regardless of the size and degree of formality adopted by a project, the process itself is usually initiated as soon as the idea for a new project has been identified during project initiation. An initial risk list or database is typically produced during project initiation and planning and is the starting point for CRM. As such, the Project Manager should designate a Risk Coordinator as early as possible to maintain and manage the risk process.

Large, complex, or unique projects tend to face a greater number of risks and require more rigor in managing risks. Regardless of the size of the project, the basic process followed for risk management (described in Section 4) is the same. However, smaller and more routine projects are not likely to require a Risk Management Committee and may not devote as much time to risk management activities.

2.3 Best Practices

The OETI project risk management vision includes the employment of best practices from both industry and the EPA. This procedure incorporates the following best practices and existing regulations and policies:

- **EPA regulations and standards**
  - EPA Directive 2100.5, System Life Cycle Management Policy. Available at http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2100.5.pdf
  - EPA Interim Agency System Life Cycle Management Procedures. Available at: http://intranet.epa.gov/otop/policies/Extended_InterimProcedures.pdf.

- **Federal regulations, industry standards, and best practices**
  - Carnegie Mellon Institute, Software Engineering Institute. Continuous Risk Management Guidebook. Available at: http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html
  - Department of Defense. Risk Management for DoD Acquisition, 5th Edition, June 2003. Available at: http://www.dau.mil/pubs/gdbks/RMG%20June%2003.pdf

- National Institute of Standards and Technology (NIST), Special Publication 800-64, Security Considerations in the Information System Development Cycle, October 2003 Available at: http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
- Office of Management and Budget (OMB) Circular A-11, Preparation and Submission of Budget. Part 7. June 2006. Available at: http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.html
- Project Management Institute - Project Management Body of Knowledge (PMBOK), Third Edition, 2004. Available at: http://www.pmibookstore.org
- Software Engineering Institute (SEI) – Capability Maturity Model® Integration (CMMI). 2002. Available at: http://www.sei.cmu.edu/cmm/

3. Roles and Responsibilities

Table 3-1 presents the roles and responsibilities for OETI project staff involved in risk management activities. The table lists functions or tasks that each project role performs. While each role is assigned to individual staff member, an individual may perform multiple roles for the project.

Table 3-1. Continuous Risk Management Roles and Responsibilities

Roles	Responsibilities
Project Manager	▪ Determines the scope of the CRM process for the project ▪ Designates a Risk Coordinator ▪ Chairs the Risk Management Committee ▪ Provides oversight or carries out overall project risk management ▪ Serves as the ultimate project authority for risk definition, planning, monitoring, control, and resolution ▪ Implements control decisions for risks and authorizes expenditure of resources for mitigation ▪ Approves all Mitigation and Contingency Plans ▪ Works with Risk Coordinator to make Risk Owner assignments ▪ Reviews and approves the reported risks, risk assessments, and action strategies ▪ Handles the communications external to the project ▪ Reviews overall risk management metrics during each quarter to evaluate CRM effectiveness
Risk Management Committee	▪ Ensures that the project performs CRM ▪ Recommends and identifies new risks to be analyzed ▪ Provides input and insight into the identified risks ▪ Facilitates the development and implementation of risk mitigation plans ▪ Assists in and performs risk identification and analysis ▪ Ensures the accuracy of probability, impact, and time frame classifications ▪ Provides recommendations for the risk assignments and responsibility for risks and actions ▪ Makes recommendations to the Project Manager for Risk Owner assignments
Risk Coordinator	▪ Plans and administers the OETI risk management process ▪ Develops or assists in identifying risks and developing risk statements (i.e., condition/impact) ▪ Assists with or performs risk analysis ▪ Facilitates the development of a risk response plan and contingency plan ▪ Participates in the Risk Management Committee meetings ▪ Communicates regularly with all task leads (government and contractor) and Risk Owner(s) to ensure coordination of all risk information ▪ Handles risk-related internal project communications by providing regular status reports ▪ Tracks and reports risk metrics on a monthly basis ▪ If a risk becomes an issue, coordinates hand over to Issue Management Coordinator
Risk Owner	▪ Develops or assists with defining the appropriate risk statement (i.e., condition/impact) ▪ Performs or assists with risk analysis ▪ Tracks risks and provides input on risk response and contingency planning ▪ Provides feedback and updates to Risk Coordinator and other staff as necessary
Risk Originator	▪ Identifies new risks for consideration by Risk Coordinator and Risk Management Committee ▪ Provides necessary details and background information about risks ▪ Remains involved in risk analysis/mitigation through the Risk Owner and Risk Coordinator ▪ Identifies where added tasks related to risk mitigation fit into project plan, if applicable

Roles	Responsibilities
	▪ Estimates time and resources required to mitigate a risk ▪ Assigns mitigation action or contingency plan to team member for implementation, as applicable
Project Team Member	▪ Identifies new risks for consideration by Risk Coordinator and Risk Management Committee ▪ Provides necessary details and background information about risks ▪ Remains involved in risk analysis/mitigation through the Risk Owner and Risk Coordinator, as necessary

4. Procedure

This section presents the process flow and steps for OETI's CRM process and describes each step of the process in detail.

4.1 Process Flow Diagram

Figure 4-1 identifies the process for CRM.

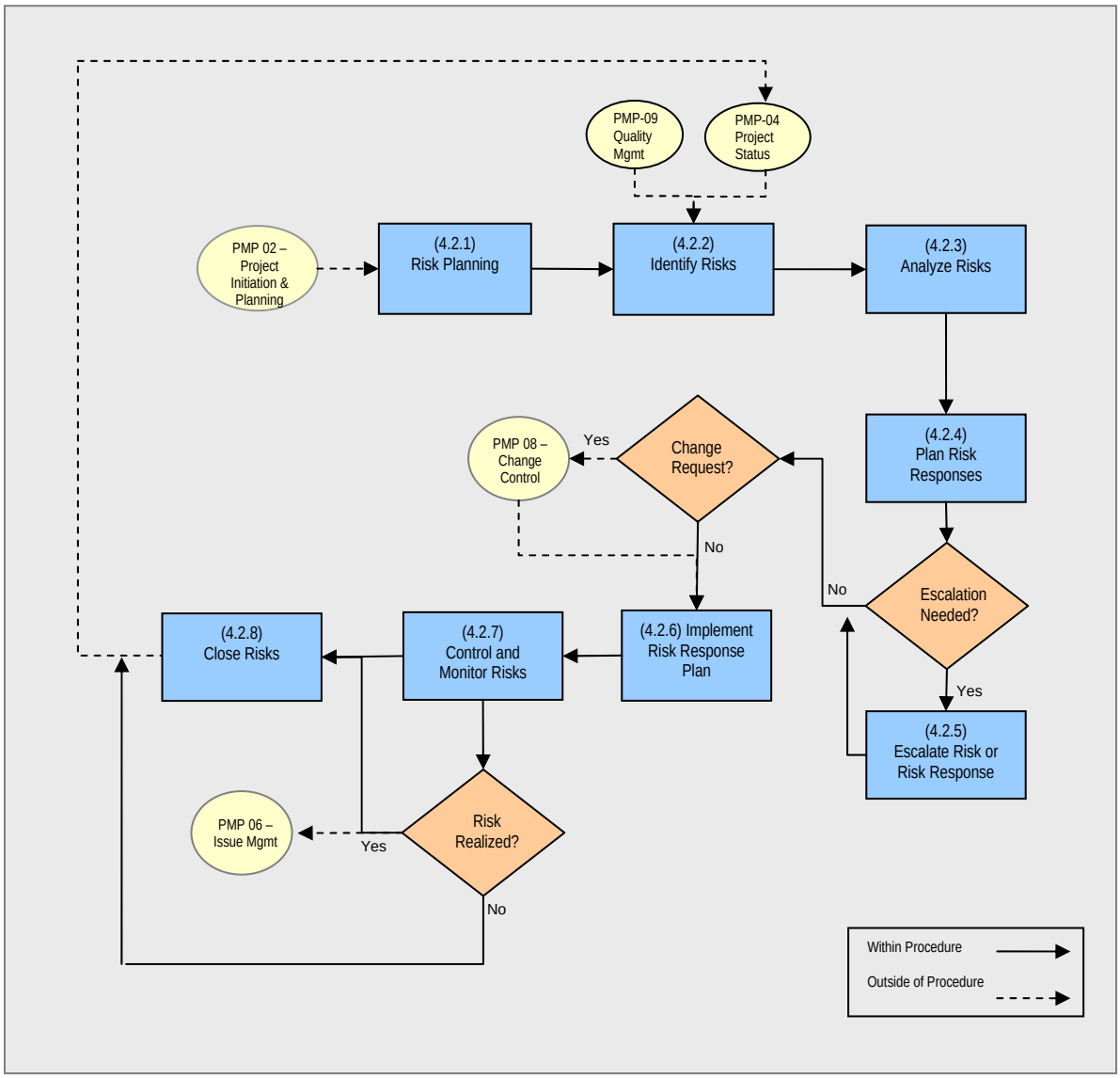

Figure 4-1. CRM Process Flow

4.2 Steps

The following sections describe the steps of the CRM process shown in Figure 4-1 and the roles involved in its execution.

4.2.1 Risk Planning

During the planning phase, the Project Manager determines the scope of the CRM process for the project. The extent of the CRM process is defined and documented in the Project Management Plan or its subsidiary plan, the Risk Management Plan (see *PMP-02 Project Initiation and Planning Procedure* for planning details). The Project Manager designates the Risk Coordinator, who is responsible for drafting the Risk Management Plan and submitting it to the Project Manager for approval. The Risk Management Plan includes the procedures, practices, and tools to be used in executing the CRM process and identifies roles and responsibilities for the execution of the CRM process. See Appendix E for a Risk Management Plan template. Planning items for risk management include:

- Scope of risk management for the project
- Methodology used for evaluating, tracking, and controlling risks
- Roles and responsibilities for scope of risk management to be implemented
- Budgeting and schedule implications for risk resources and activities
- Timing and frequency of risk management activities
- Categories used for classifying risks (may vary based on nature of project)
- Tools used for risk management and metrics to evaluate the effectiveness of risk management activities
- Reporting formats for risk tracking and reporting

The Risk Management Plan is typically developed to document the results of risk management planning activities. The Plan is a living document and is updated as needed to reflect any changes that might require restatement of the goals and objectives, scope, and processes of risk management activities. Smaller projects may document their risk management activities in the Project Management Plan as outlined in *PMP-02 Project Initiation and Planning Procedure*. As the risk management process matures, the information resulting from identifying, analyzing, and responding to risks will be incorporated into "lessons learned" and risk intelligence for future risk management activities. Project staff should receive basic training on the risk management process once risk planning activities are completed and thereafter, as necessary.

A Risk Management Committee may be established to formally manage the risk process as warranted by the size and scope of the project. In establishing the Risk Management Committee, a minimum of the following personnel or their designated representatives should be considered:

- Key Sponsor or Stakeholder(s)
- Project Manager (Chair)
- Risk Coordinator
- Project Team Leads
- Quality Assurance (QA) Manager
- Contractor Risk Manager (as necessary)
- Contractor Project Manager (as necessary)
- COR – Contracting Officer Representative (as necessary)
- Others (as necessary)

The Risk Management Committee may be chaired by the Project Manager or key stakeholder for the project. The Risk Management Committee should meet regularly, typically monthly, or as requested by the chair, to review, analyze, and assess identified risks. Project team members with specific expertise (such as the COR) may attend if there are risks that are relevant to their areas of expertise. A Risk Report or other list of risks to be covered in the meeting is usually distributed to committee members by the Risk Coordinator in advance of the meeting. Newly identified risks are collectively reviewed by the group. Once risks are accepted, risk analysis, risk mitigation strategies, prioritization, and any closures are approved by the Committee. In some cases, the Committee may determine the mitigation strategy, contingency plans, and whether escalation is required to effectively manage the risk(s). Details regarding Risk Management Committee activities and operation are defined in the Risk Management Plan.

Various EPA contractors, subcontractors, and team partners are involved in various OETI projects. These groups may be required to prepare and implement their own CRM processes. Interaction between OETI's CRM risk process and other entities' risk processes is described in Appendix D - Risk Management Interface Requirements.

4.2.2 Identify Risks

This step of the risk management process systematically identifies and validates potential risks, the factors driving risks, and documents their characteristics. Identifying risks focuses on determining what risks could impact project objectives. All project team members should be involved in identifying risks. This step builds on the initial list of risks and assumptions developed in the planning and initiation phase as described in *PMP-02 Project Initiation and Planning Procedure*. The Risk Coordinator ensures that periodic risk identification sessions are scheduled as detailed in the Risk Management Plan.

In addition to risk identification sessions, risks can be identified in several ways. Lessons learned from previous projects and experiences can provide valuable insights for identifying potential risks. The following list includes other sources that may assist in identifying risks:

- Project staff
- Trade studies
- Subject matter experts (SMEs)
- External reviewers/assessors
- Project team meetings
- Legislative or policy changes
- Status reviews and reporting mechanisms
- Approved or unapproved Change Requests (CRs)
- Quality assurance activities or results
- Project Work Breakdown Structure (WBS)

New risks are often discovered during regular status reporting activities, especially when analysis is done on schedule and dependency impacts. One purpose of quality assurance is to identify potential quality issues and mitigate them before they become problems. Analysis of quality assurance results is another source of new risks.

The mechanisms used to identify risks are described in the following sub-steps:

4.2.2.1 Submit Risk Reporting Form

Project team members, including the Risk Coordinator, Project Team Leads, and the Project Manager, along with Risk Management Committee members may identify risks and complete the Risk Reporting Form. Refer to Appendix F to view a Risk Reporting Form template. When a potential risk is identified, the Risk Originator populates a Risk Reporting Form with high-level information about the risk and submits the form to the Risk Coordinator. Alternatively, the originator may identify a potential risk during a project status or risk meeting at which time the Risk Coordinator completes the Risk Reporting Form. The following sections of the Risk Reporting Form are completed at this stage:

- Document the current date and Risk Originator name
- Assign a title or name to the risk (should be as concise as possible)
- Correlate the risk to the appropriate project WBS (if known and applicable)
- Complete the risk category, using Table 4.1 as a guide[3]

Table 4-1. Risk Categories and Indicators

Risk Category	Examples and Indicators
Strategic/Political	Cooperation between entities; stakeholder commitment; misalignment with evolving strategies; active senior management support & decision making; political changes and any resulting changes to legislation or policy; new directives from the agency or changes in priorities
Schedule	Delays in development or delivery
Business/Operational	Disruption to current business/operations, inefficient or ineffective new or existing business/operations; data and/or informational loss or disruptions; feasibility of project to be successfully accomplished in the required time frame as proposed; surety (asset protection) considerations
Technical/Technology	Inefficient design or implementation of requirements; lack of technical support; complexity of customization of code or configuration; loss of vendor, hardware, or software viability; technical obsolescence of project products; reliability of project products
Interoperability/ Integration	Interfaces or warehouse components are more complex to plan and/or develop; integration issues; dependencies on other systems or projects
Organizational Change Management	Potentially unsuccessful activities involved in (1) defining and instilling new values, attitudes, norms, and behaviors within an organization that support new ways and overcome resistance to change; (2) building consensus among customers and stakeholders on specific changes designed to better meet their needs, and (3) planning, testing, and implementing all aspects of transition from one organizational structure or business process to another
Security	Possibility that the project does not conform to applicable agency and/or federal security standards; possible violation of Privacy Act legal restrictions on the collection, use, maintenance and release of information about individuals
Staff/Project Resources	Insufficient staffing or knowledgeable resources available; sufficiently trained staff are not available; physical space; hardware shortage; lack of experienced project managers and project management tools
Cost/Budget	Sufficient funding is not available to support the planning, implementation, and/or ongoing maintenance of the system; quality of initial cost estimates and life cycle costs

[3] Risks are categorized using the definitions shown in Table 4.1, which outlines the nine risk categories OETI has identified. OETI's nine risk categories align directly to OMB's 19 risk categories that have been an integral part of the Circular A-11/Exhibit 300 data requirements (see Appendix G).

- Complete the stage field (All new risks will be in the *Initial* stage; other options include *Active* for risks in process, *Final* for risks that are ready to be closed and *Closed* stages)

After these fields are completed, the Risk Originator submits the Risk Reporting Form to the Risk Coordinator. The Risk Coordinator logs this initial information about the risk in a Risk Log. The Risk Log can be a spreadsheet or the collective fields of a tracking database of all risks and is used to document and monitor risks. The Risk Coordinator may serve as the only person who can modify the Risk Log, as directed by the Project Manager. Other models allow project team members to populate and update the Risk Log. The approach used for each project is determined in the planning stages and documented in the Risk Management Plan. Refer to Appendix H for more information on the Risk Log and its development throughout the life cycle of the project.

4.2.2.2 Determine Applicability of Risk

After submission of the Risk Reporting Form, the Risk Coordinator reviews the risk with the appropriate Project Team Member(s) to make an initial determination whether the risk is applicable to the project and that it is not a duplicate of an existing risk. If the review indicates the risk is not applicable, the decision and justification are documented on the Risk Reporting Form, the Risk Originator is notified, and no further action is taken. If it is agreed that the risk may be applicable to the project, the Risk Coordinator assigns a Risk ID and then works with the Project Manager to assign a Risk Owner, based on the Risk Owner's experience, knowledge, and his/her area of responsibility within the project team. The Risk Owner then develops and documents the risk statement that provides the supporting detail for the risk.

4.2.2.3 Document Risk Statement

The context of the risk statement should include the primary cause or condition (which may exist due to specific contributing factors, circumstances, or interrelationships) that contributes to the risk, any actions that may have been previously taken by the project to reduce or control the risk, and the potential impact or consequence should the undesired event occur, as shown in Figure 4-2[4].

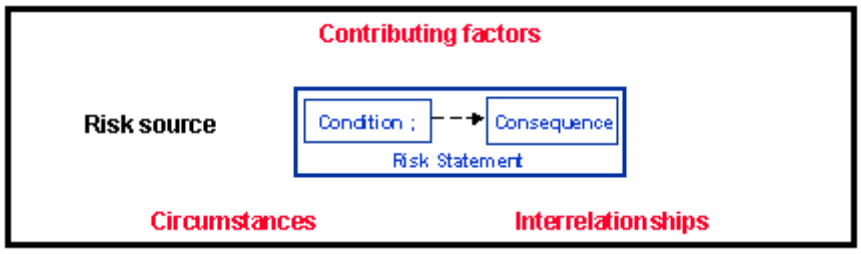

Figure 4-2: Components of a Risk Statement and Context

An example of a completed risk statement is shown in Figure 4-3[5]. Note there is one condition and two consequences in the risk statement. The context explains why this is a risk and should be included as needed to support the risk statement.

---

[4] NASA, "Continuous Risk Management at NASA" presented at the Applied Software Measurement/Software Management Conference, February 1999, San Jose, CA.

[5] Ibid.

- Risk Statement:
  This is the first time that the software staff will use Object Oriented Development (OOD); the staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.

- Context:
  OOD is a very different approach that requires special training and tends to be difficult to learn.

Figure 4-3: Example Risk Statement and Context

Following documentation of the risk statement, the Risk Coordinator may communicate with appropriate Project Team Member(s) and any contractors to obtain additional information to further clarify the risk statement.

4.2.2.4 Update Risk Log

As risk statements are defined for submitted risks, the Risk Coordinator continues to update the Risk Log or risk database as shown in Table 4-2. Table 4-2 provides an example of all risk data elements populated during the Initial stage of a new risk.

Table 4-2. Initial Risk Log Input from the Risk Identification Step

ID	Date	Risk Originator	WBS	Risk Category	Stage	Risk Owner(s)	Title	Risk Statement and Context
101	1/1/07	K. Smith	1.1 Implementa-tion	Cost/ Budget	Initial	J.Doe	SME and contractor resources	Given the Independent Government Cost Estimate, the project was based on the assumed availability of contactor and SME resources that are most likely to be unavailable, the project cost estimates and schedules may be unrealistically low, thereby negatively affecting Cost/Budget numbers and schedule

At the conclusion of each step it is the responsibility of the Risk Coordinator, in conjunction with the Risk Management Committee and/or Risk Owner, to update the Risk Log as described in this procedure.

4.2.3 Analyze Risks

The Risk Owner, in consultation with the Risk Coordinator and other relevant stakeholders (e.g., Project Team Members and contractors), performs the following steps to analyze the risk:

- Determine the impact (consequence) if the risk is realized
- Determine the probability (likelihood) of the risk occurring
- Determine the severity (or score) and classification for the risk

- Determine the timeframe for when the risk response is required based on when the risk is likely to occur
- Establish the prioritization of risk (based on the risk severity score)

These steps, described below, are performed for each identified risk to assess the range of possible project outcomes. The analysis of risks is used to prioritize risks and determine actions to be taken to respond to the risk. The Risk Coordinator continues to update the Risk Log or database on a regular basis as decisions are made for each risk.

4.2.3.1 Probability Assessment

For each risk, the Risk Coordinator and Risk Owner predict the probability or likelihood of the risk occurring. Using the probability definitions established for occurrence ratings shown in Table 4-3, the probability is assigned a value from one to five (1 – 5) and documented by the Risk Coordinator. This assessment is made based on the experience and expertise of the Risk Owner and Risk Coordinator. Additional project resources may be consulted for input if needed to make a probability determination.

Table 4-3. Probability Rating Definitions

Probability Rating	Probability of Occurrence	Perceived Likelihood the Risk will Occur
1 – Very Low	0 – 20%	Remote to little chance the risk will occur
2 – Low	21 – 40%	Unlikely to less than even chance the risk will occur
3 – Moderate	41 – 60%	About even chance the risk will occur
4 – High	61 – 80%	Likely to very good chance the risk will occur
5 – Very High	81 – 100%	Very good to near certainty the risk will occur

4.2.3.2 Impact Assessment

For each risk, the Risk Coordinator and the Risk Owner select an impact rating based on predefined impact definitions. The impact rating is determined by analyzing anticipated impacts of the risk on the project's cost, schedule, and ability to meet stated objectives. Determining the potential cost and schedule impacts of a risk is done in much the same way as the estimating and budgeting process is performed. For more information on the estimating process, refer to *PMP-02 Project Initiation and Planning Procedure* and *PMP-03 Project Schedule and Cost Baseline Procedure*. For planning purposes, the worst-case scenario is usually assumed as this information is key to determining an adequate level of project reserves.

While these are the focal points, the scope of the impact may not be limited to project cost and schedule. Additional impacts (such as impact to user buy-in or impact to staff morale) should be documented as well even though there may not be immediate estimating or contingency implications. The analysis and estimates developed are used to determine the overall impact. Table 4-4 lists the impact definitions for each impact rating. Where there is more than one appropriate impact category (such as cost/budget is low but project impact is moderate due to potential morale issues), the one with the highest impact is selected to represent the impact rating for the risk.

Table 4-4. Impact Rating Definitions

Impact Rating	Cost/Budget	Schedule	Project Impact

Impact Rating	Cost/Budget	Schedule	Project Impact
1 – Very Low	<1% cost impact or no cost impact, or increase over that allocated; can be handled within available reserves	<1% schedule impact to schedule can be handle within schedule reserve; no impact to critical path	Minor impact or no impact to project success, exit criteria, or margins. Same approach retained
2 – Low	1-2% cost increase, minor impact, can be handled within available reserves	1-2% schedule impact; can be handled within schedule reserve; no impact to critical path	Minor impact to project success or exit criteria, but can be handled within established margins. Same approach retained
3 – Moderate	3-5% cost increase; causes cost impact and use of allocated reserves	3-5% schedule impact, possibly to critical path, but can be handled within schedule reserve; no impact to milestone	Moderate impact to success or exit criteria but can be handled within established margins. Workarounds available
4 – High	6-9% cost increase; causes cost impact and may exceed allocated reserves and may require other resources	6-9% schedule impact, significant impact to critical path and cannot meet established lower level milestone	Major impact to success criteria but still meets minimum project success or exit criteria. Threatens established margins. Workarounds available
5 – Very High	10% or more cost increase, causes major cost impact and requires additional budget resources	10% or more schedule impact; causes major impact to critical path and cannot meet major milestone	Critical impact to project. Cannot meet minimum success/exit criteria. No alternatives exist

4.2.3.3 Severity Assessment and Classification

Using the probability and impact ratings for the risk, the Risk Coordinator determines the risk severity and documents it in the Risk Log. The risk severity is calculated by multiplying the probability rating by the impact rating to obtain a severity assessment score. For example, a risk with an impact of 3 (moderate impact) and probability of occurrence rating 3 (moderate probability) receives a severity score of 9. The risk severity is applied against the Risk Classification Chart shown in Figure 4-4. Based on OETI's risk tolerance, risk classifications are defined as follows:

- Red – high risks (score of 15-25)
- Yellow – medium risks (score of 6-12)
- Green – low risks (score of 1-5)

PROBABILITY					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	IMPACT				

Figure 4-4. Risk Classification Chart

In our example, the risk with a severity score of 9 is classified as a medium (or Yellow) risk. The purpose of the risk classification chart is to enable comparison of a set of risks to ascertain priority and urgency. The risks rated as Red or high severity will require immediate notification of the Project Manager to expedite the necessary resources for risk response planning.

4.2.3.4 Timeframe Assessment

The timeframe in which a risk could be realized also needs to be considered in the analysis phase and in the prioritization process. This information facilitates planning of resource requirements for managing the risk as described in Section 4.2.4. Selecting a timeframe when performing risk analysis better enables management to focus on actions required in the immediate future. Risks that may occur in the Near Term may require immediate risk response planning even if they are not classified as Red or high risk.

In some cases, a risk timeframe may not be certain or the risk could occur anytime, but the mitigation timeframe is certain. In this case, the timeframe for action may be the driver for determining the timeframe. Time frame options include the following:

- Near Term – Less than 6 months
- Mid Term – Between 6 months and 12 months
- Long Term – Greater than 1 year

The Project Manger and/or Risk Management Committee has the discretion to use the timeframe criteria to increase or decrease a risk's severity score based on its time sensitivity.

4.2.3.5 Prioritization and Reporting

Once the risk severity score is calculated and its classification determined, the risk is prioritized with other new and existing risks or within its classification. Depending on the size and complexity of the project, this may occur during Risk Management Committee meetings for larger projects or by the Project Manager or Risk Owner for smaller projects. Regardless of the forum used, this happens during regular risk review activities such as status reporting and Risk Management Committee meetings. Using the analysis provided by the Risk Owner and the classification, each risk is

evaluated within the context of the project's constraints, current status, life cycle stage, and project objectives to determine its priority. The priority assigned is used in evaluating risk response activities.

Table 4-5. Output from the Risk Analysis Step

Probability Ranking (Likelihood)	Impact Ranking (Consequence)	Risk Severity Score	Timeframe
3 = Moderate	3 = Moderate	9 = Yellow, moderate risk	Mid Term

The priority and other attributes of the risk are reviewed on a regular basis and may change over time. To facilitate the process, the Risk Coordinator produces regular risk reports. The format and extent of these reports is based on the size of the project and the Risk Management Tool used by the project. A sample Risk Report is located in Appendix I. The report formats used and the frequency of distribution are defined in the Risk Management Plan.

4.2.4 Plan Risk Responses

Once risks are analyzed and assigned a priority, the strategy for addressing the identified risks is determined. The risk response strategy is determined by the Risk Management Committee for larger projects and by the Project Manager and/or Risk Owner for smaller projects. The strategy is developed within the context of the project's constraints, current status, life cycle stage, and project objectives and is informed by the analysis performed in earlier steps of this procedure. There are four risk response strategies identified for OETI projects as described in Table 4.6.

Table 4-6. Risk Response Strategies

Response Strategy	Response Strategy Description
Avoid	Eliminate the threat by eliminating the cause (e.g., remove the work activity from the WBS that is associated with the risk)
Accept	Prepare written rationale and maintain a record of the risk in the database; development of mitigation plan is not required. However, development of a contingency plan may be considered
Transfer	Share responsibility for the risk through contract terms or outsourcing the work
Mitigate	Develop and execute a mitigation plan to eliminate or reduce probability of occurrence or impact

Note: Risks rated as Red or high severity will require immediate notification of the Project Manager to expedite the necessary resources for risk response planning.

The response strategy selected guides the project team's actions with respect to the identified risk. All strategies require some action (even if to document that no action will be taken and a justification provided). Once identified, risk response plans are documented in the Risk Log by the Risk Coordinator. An example is provided in Table 4-7.

Table 4-7. Risk Response Plan Example

Response Strategy	Activities
Transfer	Risk is transferred to X Company through the award of a fixed-price contract (Risk Owner - by March 28, 2007)

Actions taken to reduce or eliminate the risk's likelihood of occurrence and/or its impact to the project if realized are called mitigation plans. The project considers the alternative mitigation options and

develops a mitigation plan from the best option. Activities performed in developing a mitigation plan are:

- Determine goal of mitigation
- Investigate root cause of the risk and any associated risks, as appropriate
- Determine project work streams impacted
- Brainstorm options for mitigation plan
- Assess each mitigation plan option in terms of cost, schedule, and performance impact
- Choose best mitigation plan option based on goal identified
- Develop detailed mitigation steps for the selected mitigation plan
- Assign estimated completion date and responsibility for each step

However, despite best efforts, some risks may be unavoidable and will become issues that impact the project. Contingency plans describe the actions the project team may take to deal with the occurrence of these risks. Contingency plans are developed (as applicable) with appropriate triggers to initiate the implementation of the contingency.

Mitigation and contingency plans are required for all risks rated Red, or as defined in the Risk Management Plan. A contingency plan may be developed, regardless of the response strategy assigned to the risk. A contingency plan differs from a mitigation plan:

Mitigation Plan– A mitigation plan is a defined course of action or response to prevent the risk from being realized. A mitigation action is proactive rather than reactive. A risk can have both a defined mitigation and contingency plan. If the mitigation action is not effective at preventing the risk from being realized, a contingency plan may be required to minimize the consequences of the risk.

Contingency Plan – A contingency plan is a defined course of action or response that is implemented or followed to minimize or offset the impact of the risk to the project should the risk be realized. A contingency plan is not executed for a risk until the status of the risk changes and it becomes an actual issue. If the risk is effectively mitigated, the contingency plan is not implemented.

Developing a contingency plan involves the following activities:

- Identify trigger (what has to happen in order for this contingency plan to be invoked?)
- Brainstorm options for contingency plan
- Choose best alternative based on subjective input
- Develop active steps for plan
- Assign estimated completion date and responsibility for each step

Risk mitigation and contingency plans typically require additional work activities and are added to the project's WBS. New work may require a request to change the project base line. Change Requests (CRs)[6] generated as a result of risk response and contingency planning (e.g., new work, a modification to work methods, contract terms, scope, and schedule) are submitted and approved as described in *PMP-08 Change Control Procedure*. Approved CRs can generate additional risks or alter identified risks. Consequently, those changes need to be analyzed for any effects to the risk

[6] Approved CRs are the documented, authorized changes to expand or contract project scope. The approved change requests can also modify policies, project management plans, procedures, costs or budgets, or revise schedules. Approved change requests are scheduled for implementation by the project team.

response plan or Risk Management Plan. In addition, the approval/rejection of a CR may impact the timeliness of implementing the risk response plan. A rejected CR may require a different response strategy or mitigation plan. As documented in the Risk Management Plan, the Risk Owner, Risk Coordinator, and the Risk Management Committee review these items on a case-by-case basis to determine the appropriate course of action.

Implementing response strategies can bring about a secondary or residual risk. For example, buying insurance to cover unforeseen damages to a telecommunication structure is transferring the risk responsibility to the insurance company. Since "transference" is selected as the risk response strategy, the consequence of the risk is burdened upon the third party. Still, insurance may not cover all the damages should the risk occur. Remaining risks that result from implementing a risk response strategy are known as a residual risk. Also, there could be new risks based on the development of a response option. These are known as secondary risks. Both the residual risks and secondary risks will then follow the steps of the CRM (i.e., identify, analyze, respond, and monitor and control).

4.2.5 Escalate Risk or Risk Response

Occasionally the risk or the risk response, typically a mitigation action or contingency plan, may need to be escalated to senior management for approval or action. This usually occurs if the Risk Management Committee cannot implement a mitigation or contingency plan or some other response action without action or approval from more senior leader(s) and determines that escalation is needed. In this case the Committee should follow the defined escalation process in the Project Management Plan (see *PMP-02 Project Initiation and Planning Procedure* for guidance on development of the Project Management Plan). The escalation process allows for progressive tiers of management to provide input into the action or response needed until approval and/or a decision is identified. For this process step, the path of escalation should be implemented as follows:

- Project Team Lead
- Project Manager
- System or Project Sponsor
- Senior Manager or other agency official of equal or higher authority
- External government authority

The Risk Management Committee or Project Manager escalates the action item or response to the appropriate level needed to facilitate its resolution or provide the needed approval. This process differs from the change control process in that the escalation process is used to make a selection among multiple resolution options, to approve courses of action, and to negotiate with other senior managers within the organization or external vendors on behalf of the project. The project team also uses the escalation process when a specific action beyond approval or review is needed from senior management in order to move forward with risk response planning and risk management.

4.2.6 Implement Risk Response Plan

The Risk Owner is responsible for implementing the risk response actions. The risk mitigation plan must be periodically reviewed by the Risk Owner and jointly updated with the Risk Coordinator as necessary. Any updates will be presented for discussion to the Risk Management Committee or Project Manager during regular risk meetings.

4.2.7 Control and Monitor Risks

Controlling and monitoring risks focuses on determining the status of risk response activities. This step examines the results of risk response plan implementations and tracks their status. The Risk Owner and Risk Coordinator are responsible for *monitoring* the risk response implementation and its effectiveness. The Risk Owner initiates the risk response plan and notifies the Risk Coordinator of its status regularly. If the implementation of the plan is effective and eliminates the risk, rationale and justification are provided and the risk is brought before the Risk Management Committee to consider closure.

Each Risk Owner is responsible for communicating the respective status to the Risk Coordinator for documentation on a periodic basis as outlined in the Risk Management Plan. The Risk Owner provides current status and other pertinent details on each risk during the Risk Committee meetings or during regular status reporting activities. This information is captured and entered into the Risk Log by the Risk Coordinator. An example is provided in Table 4-8. All the risks identified should be consolidated and tracked on a regular basis. For a sample template of a Risk Log, refer to Appendix H. The information in this section should include:

- Status activity
- Date of status activity
- Name of person providing status, if different than the Risk Owner

Table 4-8. Monitoring and Controlling Risks: Update Status in Risk Log

Current Status and Other Pertinent Details
▪ On December 29, the Risk Committee determined that the optimal mitigation plan involves extending WBS 2.2.3 by two weeks. A CR was submitted to the CCB on December 30. Follow up meeting planned for January 7 (Ed Jones, December 30)

Based on updates from project staff and contractors, if applicable (see Appendix D, Interface Requirements, to review the methodology, process, and procedures for exchanging risk information between OETI project staff and project contractors), informed, timely, and effective decisions are made about risks and their risk response implementation plans by the Risk Committee or Project Manager. Controlling risks is integrated with and coordinated in routine project management activities. Using the Risk Log or any project risk reports generated from the Risk Log, the following are control plan decisions that are reviewed and made by the Risk Management Committee or the Project Manager:

- Continue tracking the risk as planned
- Re-evaluate the risk (increase or decrease impact, likelihood, and severity scores as applicable)
- Re-plan the mitigation or contingency actions (usually as a result of an ineffective mitigation effort or re-evaluation of the risk)
- Close the risk (either because it has been eliminated or because it has been realized)

If a risk occurs, or is realized, it becomes an issue and is closed as a project risk. When the risk is realized, the risk contingency plan will be implemented per *PMP-06 Issue Management Procedure*. For events that occur that were not identified as part of the risk management process (e.g., unknown

unknowns), the actions needed to deal with the consequences of these events are addressed in *PMP-06 Issue Management Procedure*.

The Risk Coordinator updates the Risk Log with any changes made to the status of the risk, the analysis of the risk or mitigation or contingency plans.

4.2.8 Close Risks

The process for closing risks is formal. In accordance with the Risk Management Plan, the Risk Management Committee formally reviews and approves all closed risks. Risks can be closed for a number of reasons:

- The risk is realized – the risk becomes an issue and is formally tracked and controlled through the issue management process defined in *PMP-06 Issue Management Procedure*
- Risk has been mitigated – the risk mitigation plan was implemented and successfully mitigated the risk. Analysis should be performed to determine if any residual risk(s) exist or if new risk(s) have been created as a result of the mitigation action
- Circumstances have changed – the factors contributing to the existence of the risk have changed and the risk is no longer a potential threat

As risks are reviewed and formally closed, the Risk Coordinator documents risk closure in the Risk Log.

5. Considerations

The following provides a list of general *best practices* that should be considered when conducting the continuous risk management process:

- Risk management procedures can be very general or very detailed. If the project has been completed many times before by the organization or is very small, general risk management practices may be sufficient. Large, complex, or unique projects typically require more rigorous procedures and practices.
- Large, complex projects should review and manage risks more frequently than smaller, more routine projects.
- The Project Manager, in collaboration with the project team, is always responsible for determining what risk management processes are appropriate, and the appropriate degree of rigor for each process for any given project.
- Risk management activities should include stakeholders where relevant and feasible.
- Open communication across all team members is essential to effective risk management. All team members should be provided opportunities to provide input into the risk management process as many team members are the first to be exposed to developing risks.
- Initial training and training of new team members on the risk management process may be useful for consistency and effectiveness on large and complex projects.
- Risk mitigation plans should be integrated with project plans when those plans affect project schedules, budgets, and deliverables.
- The CRM process is designed to forecast, identify, and manage risks before they become problems. As appropriate, consider lessons learned from other projects and programs to implement this procedure.
- Critical to the risk management process and development of the Project Management Plan is the analysis and understanding of the scope of the project by the Risk Management team.

Appendix A. Acronyms

Acronym	Description
ASK	Academy Sharing Knowledge
CIO	Chief Information Officer
CMMI	Capability Maturity Model® Integration
COR	Contracting Officer's Representative
CR	Change Request
CRM	Continuous Risk Management
DoD	Department of Defense
EPA	Environmental Protection Agency
NASA	National Aeronautics and Space Administration
NIST	National Institutes of Standards and Technology
OEI	Office of Environmental Information
OETI	Office of Enterprise Technology and Innovation
OMB	Office of Management and Budget
OOD	Object Oriented Design
PMBOK®	Project Management Body of Knowledge
PMI	Project Management Institute
QA	Quality Assurance
SEI	Software Engineering Institute
SIO	Senior Information Official
SLCM	Systems Life Cycle Management
SME	Subject Matter Expert
WBS	Work Breakdown Structure

Appendix B. Checklist

The following provides a checklist for the key activities associated with each step of this document management procedure.

Activity	Responsible Parties
4.2.1 Risk Planning	
❑ Risk planning is performed	Project Manager, Project Team Leads
❑ Risk Coordinator is assigned	Project Manager
❑ Risk Management Plan is completed	Risk Coordinator, Project Manager
❑ Risk Management Committee participants are determined (if applicable)	Project Sponsor, Project Manager, Project Team Leads
❑ Risk management activities are reflected in the project schedule and resources are assigned	Project Manager, Project Team Leads
❑ Risk tracking tools, metrics, forms, and reports are determined (as applicable)	Risk Coordinator
4.2.2 Identify Risks	
❑ Lessons learned from previous projects and experiences are considered to provide valuable insights for identifying potential risks	Risk Coordinator, Project Manager
❑ Risk Reporting Forms are used by project team members for each new risk identified ❑ Risk Log is populated with initial information about new risks	Risk Coordinator
❑ A project risk meeting is conducted during the early stage of the project, facilitating the identification of an initial list of project risks	Risk Coordinator, Project Manager, Project Team Members
4.2.3 Analyze Risks	
❑ Impact rating is assigned for all identified risks ❑ Probability rating is assigned for all identified risks ❑ Severity score is calculated and a risk classification determined for each identified risk ❑ Risk priority is determined ❑ All ratings, severity scores, and priorities are recorded in the Risk Log	Risk Coordinator, Risk Management Committee
4.2.4 Plan Risk Responses	
❑ Appropriate risk response strategy is evaluated within the context of the project constraints ❑ Risk response strategies for red risks are prioritized and addressed first ❑ Risk response actions are assigned	Project Manager, Risk Management Committee, Risk Owner(s)
❑ Mitigation plan is developed for each risk (if applicable) ❑ Contingency plan is developed for each risk (if applicable)	Project Manager, Risk Management Committee, Risk Owner(s)
❑ Response plan is analyzed to determine whether a Change Request (CR) is required	Project Manager, Risk Management Committee, Risk

	Owner(s)
❑ Risk and associated CR are analyzed to determine if other residual or secondary risks are introduced as a byproduct of the proposed CR	Project Manager, Risk Coordinator, Risk Management Committee
❑ WBS is updated as needed to represent risk response activities	Project Manager, Project Team Leads
❑ Risk response strategies and plans are documented in the Risk Log	Risk Coordinator
4.2.5 Escalate Risk or Risk Response	
❑ Escalation actions are determined, as applicable	Risk Management Committee, Project Manager
❑ Escalation actions are documented in the Risk Log	Risk Coordinator
❑ Actions are escalated and the outcomes are documented in the Risk Log	Risk Management Committee, Project Manager, Risk Coordinator
4.2.6 Implement Risk Response Plan	
❑ Risk response plans are implemented	Risk Owner
4.2.7 Monitor and Control Risks	
❑ Risk Management Report is prepared for regular status activities	Risk Coordinator
❑ Status of risk is communicated during status activities	Risk Owner
❑ Risk response re-planning is performed as required ❑ Alternate risk response strategy for risk is determined (as applicable)	Risk Owner, Risk Coordinator, Project Manager, Risk Management Committee
❑ Risk status changes and updates are recorded in Risk Log	Risk Coordinator
4.2.8 Close Risks	
❑ Risks proposed for closure (marked as in the Final stage) are reviewed ❑ Justifications for closing risks are approved ❑ Any associated risks that have been created as a byproduct of closing the risk(s) are determined	Risk Owner, Risk Management Committee, Project Manager
❑ Risk is recorded as closed in the Risk Log, to include accompanying justification	Risk Coordinator

Appendix C. Additional Resources

The following provides a list of key resources and references associated with the risk management procedure that can be used to obtain additional background information, describe concepts and methodologies and assist in completion of the activities. Sample templates and plans may not be directly applicable but can provide additional information helpful for applying this procedure.

	Form/ Guidance	Source	Website
1.	Guidance on developing and analyzing high level risk assessments	Washington State Department of Information Services	http://www.isb.wa.gov/tools/pmframework/precharter/riskanalysis.aspx
2.	Guidance on the execution of a Risk Management plan	Washington State Department of Information Services	http://www.isb.wa.gov/tools/pmframework/execution/risk.aspx
3.	Guidance on Acquisition Risk Management	Risk Management Guide for DoD Acquisition 2003	http://www.dau.mil/pubs/gdbks/RMG%20June%2003.pdf
4.	Guidance on Continuous Risk Management and Resources available for purchase	Software Engineering Institute, Carnegie Mellon University	http://www.sei.cmu.edu/risk/main.html
5.	Guidance on Continuous Risk Management	National Aeronautics and Space Administration (NASA) –	http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html
6.	Guidance on Continuous Risk Management and Sample Risk Log	National Aeronautics and Space Administration (NASA) – Academy Sharing Knowledge (ASK)	http://appel.nasa.gov/ask/issues/8/practices/index.html
7.	Sample Risk Implementation Strategy, Supporting Documents, Guidelines and Bibliography of Risk Best Practices	Treasury Board of Canada	http://www.tbs-sct.gc.ca/emf-cag/risk-risques/risk-risques_e.asp

Appendix D. Interface Requirements

The purpose of this appendix is to provide general guidelines for collecting the appropriate information from contractors so that all project risks identified by contractor project personnel are communicated through the risk management process defined for the project. Frequently, risk data is needed from support contractors on tasks and activities that are managed by contractors. In addition, defined interface points ensure that both the government and contractor understand their specific roles and responsibilities in risk management and that the information can be efficiently captured using the project's established management processes and tools. As a result, the data, reporting, and interface requirements should be well defined early in the process to ensure that they are fully described in the awarded contract. For risk management, these requirements may include the contractor's role in the risk management process, required inputs to the process, or resulting risk response actions.

The following series of questions is provided to help determine the risk management interface requirements appropriate for a specific project. Requirements may vary significantly depending on the scope, complexity, size, and duration of the project and type of contracts awarded. Overall, the questions are designed to help refine what kind of information will be needed to ensure effective risk management of the project and to define the correlating responsibilities of the contractor.

- Will the contractor be required to develop a risk management plan for managing their work on the project? How and to what extent will their plan and process be required to comply with this risk management procedure?
- Will the contractor be able or required to identify risks and submit Risk Reporting Forms or another risk identification tool?
  - What level of detail is needed on the risk form?
  - What data elements must be provided?
  - Will the contractor need training or guidance on how to identify and submit a risk?
  - Will the contractor need access to a specialized tool or site for accessing and submitting risks?
  - Will the contractor be likely to be assigned a risk (be a Risk Owner)?
  - Will the contractor be required to submit documentation to support (such as cost and schedule impacts) the risk impact ratings?
- Will the contractor be required to act as a Risk Coordinator or participate on the Risk Management Committee?
- Does the contractor have specific subject matter expertise that may require their participation in risk response strategy planning and actions?
- Will the contractor have a role in the risk escalation process?
- Will the contractor potentially be assigned additional work under a new/existing WBS as a result of risk mitigation or a contingency plan?
- Will the contractor be evaluated based on ability to identify and plan for project risks?
- How will the contractor be involved in risk communication and status activities?
- Will the contractor be required to identify internal risks that may impact overall project performance and may not be readily apparent to other members of the project team?

Appendix E. Risk Management Plan Template

The Risk Management Plan describes how the project handles risks and describes each of the risk processes (identify, analyze, respond, and monitor and control) to be implemented, monitored, and controlled throughout the life of the project by addressing any potential risk to the successful acquisition, implementation, maintenance, and operation of project. At a minimum, the risk management plan should contain the following elements:

- Methodology. This section describes the procedures, practices, tools, and data sources that will be used to employ risk management.
- Roles and Responsibilities. The roles of all major stakeholders as they relate to the risk management process should be defined. The resources required to meet risk planning objectives are currently identified, assessed, and requested for approval and allocation.
- Budgeting. This section contains information on the resources and estimated costs needed to support risk management activities for the project. These risk management activities should be included in the project cost baseline. Projects that have high severity or numerous risks with high impact and occurrence may require additional funds for managing risks. More information on cost estimating is provided in *PMP-02 Project Initiation and Planning Procedure*. These estimates are for the CRM process only and not individual risk mitigation plans.
- Timing: This area within the risk management plan defines the frequency of the risk management process activities.
- Risk Categories: Describes how the project defines the categorization of typical risks. The risk categories may be revisited during the risk identification process.
- Reporting and tracking formats. The mechanism for recording and tracking risk and risk response plans should be discussed.

A sample template follows on the next page:

Risk Management Plan Template

This appendix provides a sample Risk Management Plan template that may be used and/or tailored as appropriate according to project needs. Appendix C provides Internet links to other examples of risk management plans and approaches.

Risk Management Plan Template

Acceptance / Approval Page

DOCUMENT CHANGE HISTORY – *Complete the version, date, author and description column to accurately describe the modifications made to this document.*

Version	Date	Author	Description of Changes
V X.X			

1.0 INTRODUCTION

[Briefly describe the purpose of the Risk Management Plan, e.g., to describe the processes that will be used to identify and evaluate risks, and to pro-actively develop strategies to reduce the probability and impact of risks. Discussion could include background on OMB and EPA requirements as well as why risks are important to identify and manage for this specific project.]

2.0 RISK MANAGEMENT METHODOLOGY

[Describe the methodology used to manage risks for this project. This includes the activities and tools that are part of the risk management processes. Risk is managed by identifying, assessing, mitigating, and tracking potential threats to project success.]

3.0 ROLES AND RESPONSIBILITIES

[Describe roles and responsibilities for performing risk analysis and risk response throughout the project life cycle. This includes establishment of a Risk Management Committee and any guidelines for its operation, if applicable.]

Based on the scope of the project, these activities may focus on project management, systems development, software testing, and systems integration. The risk management activities to be performed by the team will also include but will not be limited to conducting/participating in regularly scheduled project status reviews, milestone reviews, systems development lifecycle reviews, and evaluating and reporting on project performance. These risk management activities will also involve identifying and implementing risk reduction measures. Also, please provide background on the experience, any certifications, etc. of the team members who will be taking on key roles and responsibilities.

4.0 RISK IDENTIFICATION

[Describe how risks will be identified. Include the frequency and format of risk identification procedures. The risks should be categorized in an appropriate manner specific to the project.]

5.0 RISK ANALYSIS

[This analysis involves describing the risk, estimating its impact, and estimating the probability of occurrence. This section should also define how a severity rating is determined and the risk classification scale used, if applicable.]

6.0 RISK RESPONSE PLANNING

[Describe the process of planning and implementing action to lessen the impact or probability of a risk event. This section should also discuss the escalation process.]

Specific tasks for controlling a risk are defined based on a risk management strategy that considers the severity of the risk, project goals, and resource considerations. Possible risk management strategies include:

- Avoid - Take action to reduce the probability of risk occurrence
- Transfer – Accept the risk but reduce the impact by sharing the costs with others
- Mitigate – Take action to reduce the impact of the risk event
- Accept – Accept the consequences of the risk if it is realized.

Describe potential risk mitigation strategies that have been reviewed and approved by the team leaders and the project manager following the risk assessment process.

7.0 RISK MONITORING AND CONTROL

[Describe the process that will be used to monitor and control risks. Criteria used to close and change risk status should also be defined.]

Risks can be monitored and controlled in many ways and formats. Within risk monitoring and control there are many roles and responsibilities. The Project Manager generally manages and monitors the Risk Owners while highlighting risks that are beyond project control. The Project Team members assist in implementing risk response plans under the direction of the risk owners. The Project Sponsors provide oversight while the senior executives/management assist in managing risks outside of direct project control, champion the project, and defend it against internal and external threats. Lastly, the Risk Owner is primarily responsible for the execution of risk response and contingency plans and the overall management of their assigned risks throughout the life cycle of the risks.

Appendix F. Risk Reporting Form

The Risk Reporting Form contains the following data elements:

- Risk ID: As the Risk Coordinator receives the risks from each project team member, a unique identifier is assigned.
- Date: Indicate the date (MM/DD/YY) the risk was first identified.
- Title: A short description of a risk. The details of the risk should be indicated in the risk statement.
- Work Breakdown Structure (WBS): Assign the risk to the WBS item that is affected. Indicate the number and title of the WBS.
- Risk Originator: The individual who first identifies the risk and submits the initial Risk Reporting Form.
- Category: A one-word or short statement description of the risk (i.e., Security, Cost/Budget, etc). Risk categories can be found in Table 4-1.
- Risk Assigned To (Risk Owner/s): The person(s) responsible and accountable for the action.
- Assigned Date: Date the risk is formally assigned a risk owner(s).
- Risk Statement and Context: Should contain the risk statement and be a succinct cause-and-effect description of the risk. It should include primary causes and contributors to the risk (context), any actions that may have been previously taken by the project to reduce or control the risk, and the potential impact should the undesired event occur. The following is an example of a risk or condition/impact statement: "The project originally estimated building Module-A will take *x* amount of time and our more current projections indicate it will take *x+15* days, it is possible Module-A delivery will be delayed by 45 days, which can negatively affect the critical path."

A sample of the Risk Reporting Form is found below.

RISK REPORTING FORM

Risk Reporting Form		
Risk Identification		
Risk ID:	**Date:**	**Risk Title:**
WBS (correlated to risk):	**Risk Originator:**	**Risk Category:**
Risk Assigned To (Risk Owner/s):	**Assignment Date:**	
Risk Statement and Context:		

Appendix G. Risk Category Alignment with OMB Exhibit 300

The following list presents the nineteen risk factors as presented in past Exhibit 300 submissions. In addition, Table G-1 contains a crosswalk of the OMB categories to the OETI Risk Categories. *Definitions of the 19 categories (or areas) of risk are as follows:*

1. **Schedule:** Risk associated with the adequacy of the time estimated and allocated for the development, production, fielding, operations, maintenance, and disposal of the system. Two risk areas bearing on schedule risk are (1) the risk that the schedule estimates and objectives are unrealistic and unreasonable and (2) the risk that program execution will fall short of the schedule objectives as a result of failure to mitigate technical risk and external constraints.

2. **Initial Cost:** Risk associated with an incomplete or inaccurate cost estimate at the start up of the investment and including planning and/or sunk costs associated with the change of direction of an investment.

3. **Life-Cycle Costs:** Risk associated with the ability of the system to achieve the program's life-cycle cost objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined). This includes planning, development, operations, and retirement costs.

4. **Technical Obsolescence:** Risk that strategies for avoiding the use of outdated technical resources over the system life are not planned for and implemented. A plan for regular technology upgrade or refresh is one way to avoid obsolescence by ensuring the use of advanced versions of equipment or software when they become available.

5. **Feasibility:** Risk of insufficient ability to successfully develop and implement the investment within defined technical, scope, cost, and schedule parameters to successfully meet the performance goals due to unrealistic goals, unavailable/unproven or immature technology, lack of expertise, underdeveloped concepts, changes in the external environment, and other related factors.

6. **Reliability of Systems:** Risk of technical problems/failures with applications and associated product support and their ability to provide planned and desired technical functionality as needed and expected.

7. **Dependencies and Interoperability Between this System and Others:** Risk associated with the reliance on technical interfaces with other systems (existing or in development) within the agency and across the federal government. Risk is increased if the success of an investment is directly linked to the success/implementation or on-going maintenance of other systems.

8. **Surety (Asset Protection) Considerations:** Risk associated with the impact of loss, damage, or theft and the adequacy of physical protection, continuity of operations, and disaster recovery plans, and operations for the system.

9. **Risk of Creating a Monopoly for Future Procurements:** Risk associated with the use of closed or proprietary software/source code, as well the dependence on a single vendor or product.

10. **Capability of Agency to Manage the Investment:** Risk associated with the existence of an experienced project management team, appropriate project management structures,

executive management support, governance, clear and defined responsibilities, as well as demonstrated experience in managing investments of similar size and scope. Also relates to the degree to which program plans and strategies exist and are realistic and consistent.

11. **Overall Risk of Project Failure:** Risk associated with the negative impact resulting from the occurrence of one or more identified or unidentified risks, leading to catastrophic results for the investment. It refers to the aggregation of identified risks associated with this investment and the likelihood (probability and impact) that one or more occurrences of risk will cause this investment to fail. It also includes the risk that unidentified risks (e.g., change in strategic direction) occur, leading to the investment becoming obsolete.

12. **Organizational and Change Management:** Risk associated with organizational/agency/ government-wide cultural resistance to change and standardization; risk associated with bypassing, lack of use or improper use or adherence to new systems and processes due to organizational structure and culture; inadequate training planning.

13. **Business:** Risk associated with business goals; risk that the proposed alternative fails to result in process efficiencies and streamlining; risk that business goals of the program or investment will not be achieved; risk that the program effectiveness targeted by the investment will not be achieved.

14. **Data/Information:** Risk associated with the loss/misuse of data or information, risk of increased burdens on citizens and businesses due to data collection requirements if the associated business processes, or the investment, require access to data from other sources (federal, state, and/or local agencies).

15. **Technology:** Risk associated with immaturity of commercially available technology; reliance on a small number of vendors; risk of technical problems/failures with applications and their ability to provide planned and desired technical functionality. Technical risk addresses the possibility that the application of software engineering theories, principles, and techniques will fail to yield the appropriate software product. Technical risk is comprised of the underlying technological factors that may cause the final product to be: overly expensive, delivered late or otherwise unacceptable to the customer.

16. **Strategic:** Risk associated with strategic/government-wide goals (i.e., President's Management Agenda and e-Gov initiative goals) - risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them. Risk that the objectives of the investment are not clearly linked to program needs, to the agency's overall strategies, and to government-wide policies and standards. Risk that the investment is not based on clearly understood needs or opportunities and is inconsistent with the overall strategies and architectures used by the agency and the federal government (i.e., Federal Enterprise Architecture).

17. **Security:** Risk associated with the security/vulnerability of systems, websites, information and networks; risk of intrusions and connectivity to other (vulnerable) systems; risk associated with the misuse (criminal/fraudulent) of information. *[Note: This area must include level of risk (high, medium, and basic/low) and what aspect of security determines the level of risk, e.g. need for confidentiality of information associated with the investment/system, availability of the information or system, or reliability of the information or system.]*

18. **Privacy:** Risk associated with the vulnerability of information collected on individuals, or the risk of vulnerability of proprietary information on businesses.

19. **Project Resources:** Risk associated with "cost creep," incorrect estimation of lifecycle costs, reliance on a small number of vendors without cost controls, (poor) acquisition planning. Addresses the adequacy of people, funds, schedule, and tools as necessary ingredients for successfully implementing the investment (if any are inadequate, to include the qualifications of the people, there is risk).

Table G-1 Risk Category Cross Reference Chart – OMB 300 (19) to OETI (9)

No.	OMB 300 CPIC Risk Category	OETI Risk Category
1	Schedule	Schedule
2	Initial Costs	Cost/Budget
3	Life Cycle Costs	Cost/Budget
4	Technical Obsolescence	Technical/Technology
5	Feasibility	Business/Operational, Cost/Budget
6	Reliability of Systems	Technical/Technology
7	Dependencies & Interoperability Between this System and Others	Technical/ Technology, Interoperability/Integration
8	Surety	Schedule, Business/Operational
9	Risk of Creating Monopoly for Future Procurements	Strategic/Political, Business/Operational
10	Capability of Agency to Manage the Investment	Staff/Project Resources
11	Overall Risk of Investment Failure	Strategic/Political
12	Organizational and Change Management	Organizational Change Management, Strategic/Political
13	Business	Business/Operational, Strategic/Political
14	Data/Information	Technical/Technology, Interoperability/Integration
15	Technology	Technical/Technology
16	Strategic	Strategic/Political
17	Security	Security, Technical/Technology
18	Privacy	Security, Technical/Technology
19	Project Resources	Staff/Project Resources

Appendix H. Risk Log

This appendix provides a sample Risk Management Report. The format may vary by project depending on the tool(s) used and the extent to which risk management processes are implemented for the project. Sections of the Risk Log are completed at various stages of the risk management process. Fields included on the Risk Log include all those found on the Risk Reporting Form as well as the following:

- Probability Rating: The likelihood that the risk will occur. This rating is typically assigned by the Risk Owner with possible input from the Risk Coordinator or Risk Management Committee.
- Impact Rating: The impact to the project should the risk actually occur. This rating is typically assigned by the Risk Owner with possible input from the Risk Coordinator or Risk Management Committee.
- Risk Severity Score: The overall risk rating which is calculated by multiplying the probability rating by the impact rating. The higher the number, the more severe the risk.
- Risk Timeframe: The timeframe in which the risk is most likely to occur if it is realized. If the timeframe is unsure or if it is a risk that spans timeframes, it is the timeframe in which risk response planning/action is required.
- Response Option: Indicate the category of risk response that actively and directly handles risks before they are realized.
- Areas Affected by Risk: Identify the areas, activities or groups impacted by the risk if it is realized.
- Current Status/Updates: Field is updated as a result of status activities and Risk Management Committee meetings as status changes. The information in this section should include: status activity, date of status activity, and name of person providing status.
- Actions: Record any actions taken specifically to address the risk; include detailed information regarding project plan activities, resources involved, etc.
- Related Risks: Document any risks identified that are related to this risk or were created from action(s) taken for this risk.
- Business Impact Analysis: Document any business impacts identified during impact assessment of the risk.
- Root Cause Analysis: Provide any additional details regarding the cause of the risk (as needed).
- Cost/Budget Impact: Provide documentation for cost impacts identified during the impact assessment of the risk.
- Schedule Impact: Provide information regarding any schedule impacts identified during the impact assessment of the risk.
- Other Impacts: Provide information for any other potential impacts of the risk that were identified during the impact assessment for the risk.
- Mitigation Plan: Provide the details of the mitigation plan (if applicable).
- Contingency Plan: Provide details for the contingency plan for the risk should the risk be realized.
- Mitigation Data: The last section of the form is for capturing information related to the effectiveness of the mitigation strategy/plan, if one was implemented for the risk.

Sample Risk Log

Risk ID	Date	Title	WBS	Originator	Category	Stage	Owner(s)	Assignment Date	Risk Statement	Probability (Likelihood)	Impact (Consequence)	Severity Assessment Score	Timeframe	Response Option	Areas Affected	Current Status	Action(s)	Related Risk	Business Impact Analysis	Root Cause Analysis	Budget/Cost Impact	Schedule Impact	Other Impacts	Mitigation Plan	Contingency Plan	Mitigation Plan	Mitigation Data

Appendix I. Risk Management Report

This appendix provides a sample Risk Management Report. The format and number of reports may vary by project depending on the tool(s) used and the extent to which risk management processes are implemented for the project.

Sample Status Report
(Date Here …)

- Risk Management Committee met (Date Here….) Agreed-upon and accepted items include the following:
  Closed - 3 Yellow and 1 Green (Details here..)
  New - 2 Yellow identified (Details here …)
  Updates – 4 existing risks received updates (Details Here)
- Current risk list has 7 open risks (down from 11 last week) as follows:

		Risk Type			
Group	**Total Risks**	**R**	**Y**	**G**	**NA***
Group A	2	1	1	-	-
Group B	2	-	1	1	-
Group C	2	1	1	-	-
Group D		-	-	-	-
Group E		-	-	-	-
Group F			-	-	
Group G		-	-	-	-
Group H		-	-	-	-
Group I		-	-	-	-
Other (Group X)	7	-	-	1	-
Risk Totals	7	2	3	2	-

*N/A - Draft in discussion

Status & scoring for Red Risk, ID # xyz sample, Title: abcedefg

- Details Closed Here...
- Details Open Here …
- Details Other Here

Distribution List:
AB@epamail.gov
BC@epamail.gov
etc