Managing Capital Investments at the Indian Health Service

A “How-To” Guide to
Risk Management

February 2013

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

ACKNOWLEDGEMENT

The Indian Health Service gratefully acknowledges the assistance of the National Institutes of Health, Office of the Deputy Chief Information Officer, in the preparation of this document.

Document Change History

Version Number	Release Date	Summary of Changes
1.0	July 14, 2006	Initial release
2.0	February 14, 2013	Updated document to be consistent with the Department of Health and Human Services Project and Portfolio Management tool and added questions to assist in the risk assessment.

Contents

Figures

A “How-To” Guide to Risk Management

PURPOSE

This guide is intended to be used by project managers and project team members to manage the risks associated with their projects.[1] The purpose of this guide is to provide a basic, easy, step-wise method for managing the risks associated with a project; a method that is consistent with federal and Indian Health Service (IHS) requirements. *A Guide to the Project Management Body of Knowledge (PMBOK Guide),* ANSI/PMI 99-001-2008 published by the Project Management Institute can provide a more comprehensive reference guide.

All information technology projects have risk. Risk management provides a means to identify the potential problems before they occur. Activities addressing these problems are planned and executed, as needed, across the life of the project to mitigate adverse impacts on achieving the project’s objectives. The purpose of Risk Management is to proactively identify and manage potential problems that may occur during a project’s implementation lifecycle. Risk management is a continuous process that will occur throughout the project lifecycle. Effective risk management includes early and aggressive risk identification through the collaboration of relevant project stakeholders.

The output of this process is a risk management approach to be used as part of the overall project management process.

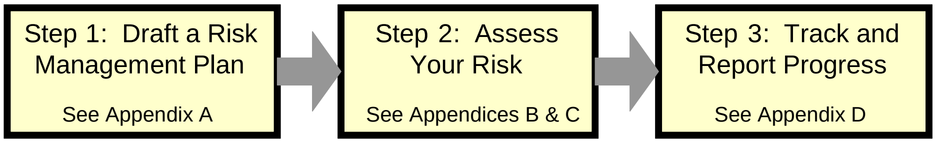
This process describes the following four activities and the steps involved in these activities:

- Identify and analyze risks early and determine their relative importance.
- Provide a tracking system to document, monitor, and update risks systematically.
- Manage risks by handling them appropriately.
- Make timely and appropriate decisions based on risk assessment and monitoring.

This guide first presents the basics of risk management, defining the terms and then providing a step-by-step approach to managing risks, following the steps shown in Figure 1.

[1] OMB uses the term “investment” to incorporate the projects, programs, systems, etc., that fall under the purview of the Capital Planning and Investment Control (CPIC) process. Because this guide supports the CPIC process, in this document, this document uses the term “project” to be synonymous with the term “investment.”

Figure 1. Overview of Risk Management



Appendix A contains a template for a draft risk management plan. Appendix B tells how to conduct a comprehensive risk review and Appendix C contains an example of a comprehensive risk review.

THE BASICS

What Is Risk?

A risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective, such as time, cost, scope, or quality. A risk may have one or more causes and one or more impacts.[2] For reasons of simplicity, we are only considering risks with negative outcomes. A risk is any factor that has the potential to interfere with the successful completion of the project. Risks are not events that have already occurred, but events that might occur and that have the potential to adversely impact the project in some way..

What Is Risk Management?

Risk management is an organized method of identifying, prioritizing, and measuring the impact of project risks and developing, selecting, and managing options for handling those risks—not necessarily to eliminate them entirely, but to minimize their impact on the project.

Managing project risk is a key component of good project management. Risks that are managed are minimized. Understanding and communicating risks help manage the expectations of senior management and other stakeholders. One such stakeholder, the Office of Management and Budget (OMB), requires a formal risk management plan for major projects and has in the past required annual reporting of risks and risk mitigation progress before approving requested project funding.[3]

[2] *A Guide to the Project Management Body of Knowledge*, Fourth Edition (PMBOK Guide), ANSI/PMI 99-001-2008, Project Management Institute, Inc, Newton Square, PA, 2008.

[3] OMB does not specify a risk management plan format or content, but the previous reporting requirements of the Exhibit 300 imply obvious plan elements. These elements are also selection elements in the ProSight tool.

How Do You Manage Risk?

The appropriate level of risk management for any project depends on many factors (e.g., size, complexity, life-cycle phase, and stability) and determining that level requires candid management judgment. For example, a stable, straightforward application using established technology in the maintenance phase of its life cycle needs a far less extensive risk management program than a large, complex agency-wide system just beginning the development phase.

No one risk management approach is appropriate for all projects. Managers of smaller projects can profitably use elements of these risk management guidelines without the administrative burden of reporting risks to OMB. Those subject to OMB or HHS oversight *must* satisfy OMB requirements; risk status and mitigation must be well documented to be assured that the project manager is managing risks sufficiently well that project success is probable.

DRAFT A RISK MANAGEMENT PLAN

The risk management planning process begins with the selection of a risk management process model. One such model is shown in Figure 2. The risk management process model in Figure 2 is straightforward, and its elements are readily adaptable to the range of projects at IHS. The first four activities of the risk management process model depicted in the figure, designated as the planning phase and presented in the top row, specify the actions required to complete Step 2 of Figure 1, *Assess Your Risk*. The last three activities of the risk management process model, designated as the execution phase and presented in the bottom row of the figure, specify the actions required to complete Step 3 of Figure 1, *Track and Report Progress*.

Step 1: Draft a Risk Management Plan

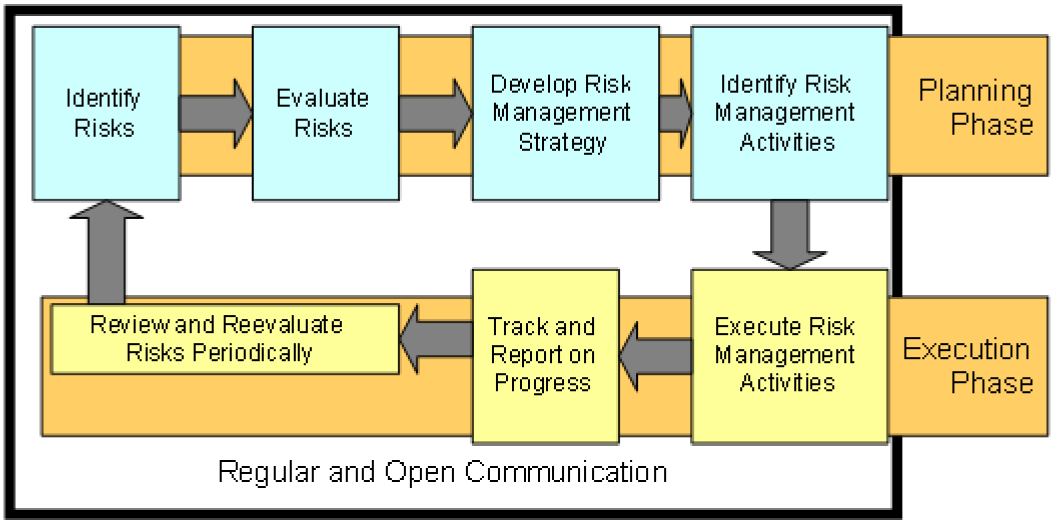
See Appendix A

To draft a plan for your project, you will have to consider what level of detail is required to identify risks, what methods are appropriate for evaluating the risks, who will be responsible for developing strategies to manage the risks, and how risk management actions will be developed, monitored, and reported. The level of funding, impact, or complexity of a project will determine how fully and detailed the risks are identified, managed, and tracked.

When completed, the risk management plan for your project should be dated and published. It should be made available to all project personnel, oversight and audit personnel, project sponsors, and other interested stakeholders.

A template for a risk management plan is presented in Appendix A.

Figure 2. The Risk Management Process


Identify Risks
Evaluate Risks
Develop Risk Management Strategy
Identify Risk Management Activities
Planning Phase
Review and Reevaluate Risks Periodically
Track and Report on Progress
Execute Risk Management Activities
Execution Phase
Regular and Open Communication

Assess Your Risk

Step 2: Assess Your Risk

See Appendices B & C

The planning phase of the risk management process model provides an assessment of project risks, including understanding the nature, likelihood, and potential impact of risk. It has four discrete elements:

- *Identify risks.* The risks inherent in your project should be defined in two ways: (1) they should be part of a continuous, ongoing part of project management so that risks are managed as risks arise; and (2) there should be a periodic, independent, comprehensive assessment of potential risks to assure that potential new risks are fully identified and managed.

  As discussed in Appendix B, OMB has identified 19 risk categories, that provide a minimum set of risk areas to be considered by the project risk assessment team:

  1) Schedule

  2) Initial cost

  3) Life-cycle cost

  4) Technical obsolescence

  5) Feasibility

  6) Reliability of systems

  7) Dependencies and interoperability

  8) Surety (asset protections)

  9) Risk of creating a monopoly

10) Capability of agency to manage the investment
11) Overall risk of investment failure
12) Organizational and change management
13) Business
14) Data/information
15) Technology
16) Strategic
17) Security
18) Privacy
19) Project resources

- *Evaluate risks.* Once the risks have been identified, the Project Team will analyze those risks by determining how they might impede the overall success of the project if they occur. Each risk should be rated in terms of (1) the likelihood that the risk will occur and (2) its potential impact on the project if it does occur. This rating can be expressed as high, medium, or low for both probability of occurrence and for the potential impact. Then, a level of magnitude can be computed by assigning a numerical score to each risk by multiplying the numerical score of the risk's likelihood of occurrence by its potential impact score. By formally evaluating the risks in this way, the project team can determine how each risk should be managed, depending on its magnitude. Risks with a high magnitude should receive greater management attention than those with a low magnitude.

  Risks with a high magnitude represent those risks that are deemed to pose the greatest threat to program success and accomplishment, i.e., the high-risk items. These items are typically reviewed at all internal program status reviews. Once a high magnitude risk is sufficiently mitigated that it can be closed out, it is reduced in priority and moved to an appropriate spot on the watch list. Caution must be exercised when closing out any risk from the high magnitude list. Closure does not mean file and forget. A closed risk may resurface and should continue to be observed, tracked, and documented.

  After quantifying each high magnitude risk, the risks should be prioritized from the most to least important. This allows the team to focus on the most important risks first.

  The Risk Assessment process should begin with the project team; however, all project stakeholders should have input. During regularly scheduled risk reviews, the project team will reassess risks previously identified, as well as newly identified risks.

- *Develop risk management strategy.* The most appropriate strategy for managing each risk should be determined. If a negative risk can be avoided (e.g., changing the project plan), if it is transferred (e.g., through the use of a firm fixed-price contract), or if it is accepted (e.g., there is no other suitable response strategy), it need no longer be part of the on-going risk management strategy, although it should be identified and the action taken on documented. The remaining risk management strategy for a negative risk should be to develop a mitigation strategy, which is what you do to try to keep the risk from occurring in the first place. For a positive risk (i.e., an opportunity), the risk management strategy may include exploiting it by insuring that the opportunity will definitely happen; sharing or transferring it to another organization that can best take advantage of it; or enhancing it or increasing the probability of the opportunity occurring. Regardless of whether the risk is positive or negative, if it is of medium or of high magnitude, you should also develop a risk management strategy or contingency plan, which is what you plan to do if the risk occurs.

  The risk management strategy is expressed in a short statement that describes the approach to managing the risk. For a risk with a high magnitude, a specific risk owner may be assigned to manage the risk and its mitigation activities. For negative risks that cannot be mitigated or which are too expensive to mitigate, a risk response or contingency plan should be developed and documented in the risk log. The risk management strategy, along with any related work, e.g., controls, should be agreed to via consensus techniques.

  Acceptable risk management options are:

  - **Accept –** Accept the risk when there are no viable options to mitigate or avoid the risk, or where the management or avoidance of the risk is not economically practical. In situations where nothing can realistically be done to prevent a risk from happening, the project risks should have a higher degree of scrutiny so that the probability or impact of occurrence is minimized. The Project Sponsor will formally accept the potential impact of this risk on the project. There may be contingency plans or reserves developed for these types of risks. A contingency plan is a pre-defined action that can be implemented in the event that a previously identified risk occurs, in order to diminish impact on the project (i.e., "What should the team do if…?").
  - **Manage -** Reduce the expected impact associated with the risk through mitigation and contingency techniques. Mitigation is a preventative action, e.g., controls, that are performed to reduce the probability of the occurrence, increase the visibility of the risk, or reduce the seriousness of the impact should the risk occur (i.e., "What should the team do now to minimize or prevent the risk and to minimize its impact?"). There is usually a cost associated with a risk mitigation

approach. The estimated cost of such mitigation should be identified and documented in the Risk Log. Contingency outlines a “plan of action” to take if the risk occurs and becomes an event to be dealt with.

  - **Avoid -** Eliminate the impact of the risk upon the project by formally transferring this risk to another party. This is usually accomplished through some form of contractual agreement.

- *Identify risk management activities.* The project manager, or risk owner if one is assigned, should develop an approach and action plan to implement the risk management strategy.

A guide for conducting an open and comprehensive risk review is presented in Appendix B and an example of a comprehensive Risk Log is contained in Appendix C.

TRACK AND REPORT PROGRESS

The execution phase of the risk management process model provides a periodic review of the status of risk management activities. Tracking and reporting progress on the actions taken to manage the risks include both monitoring the progress toward mitigating the risk and periodically reassessing risk..

Step 3: Track and Report Progress

See Appendix D

Executing Risk Management Activities

Overall execution of the risk management strategy and the corresponding management activities is managed by the risk owner. Risk management status is tracked against the planned risk management activities developed for each risk. HHS uses a commercial software package, currently Primavera ProSight, as its portfolio management tool (PMT) to track information technology investments that are subject to HHS review. The PMT provides forms to use for reporting project risks, their levels of magnitude, and their risk management strategies.

Reporting Risk Management Progress

Risk owners regularly report on their progress in implementing the risk management strategies and the current status of the risk management activities. These reports are presented to the other members of the project team at a level of detail commensurate with the risk magnitude and in the format prescribed by the project manager.

Progress may also be reported regularly to senior management outside the project team if appropriate.

Examples of reporting measures to be used can include:

- Number of risks identified, managed, tracked, and controlled.
- Monitoring the indicators that will trigger thresholds.
- Risk exposure and changes to the risk exposure for each assessed risk (as a summary percentage of management reserve).
- Change activity for the risk (e.g., processes, schedule, funding).
- Occurrence of unanticipated risks.
- Risk categorization volatility.
- Comparison of estimated versus actual risk management effort and impact.

Earned value management metrics can be used as “risk triggers” to predict when cost and schedule risks are likely to occur or whether they are sufficiently under control. Most projects are required to use earned-value management to track and report on cost and schedule performance. HHS has developed a three-tiered definition of projects that are required to report cost and schedule variances.

Reevaluating Project Risk

A comprehensive review and assessment should occur frequently, as determined by the Project Manager, but at least once per year. Reviews can be timed to provide current comprehensive information to assist the project manager with preparing reports, and as a minimum, for the annual IHS or HHS business case review and prioritization process.

During the reevaluation process, it may be determined that some risks that were identified in past evaluations, or as part of the ongoing risk identification process, have been successfully mitigated. These risks should still be listed on the risk inventory with an annotation that no action is necessary, the risk has been successfully mitigated. This will demonstrate that the risk was identified and managed at some time as part of the risk identification and assessment process.

Conducting Lessons Learned Sessions

The lessons learned activity involves determining the causes of variances in performance, the reason behind corrective actions chosen, and project activities that worked well and those that did not. Lessons learned should be documented as part of the historical record for the current project and as a “best practice” reference for future projects. The lessons learned review should be conducted following completion of each major lifecycle phase. At a minimum, projects perform a lessons learned review at the end of each phase and at project completion.

A lesson learned session serves as a valuable phase closure activity. The session provides an opportunity for public praise and recognition for project team members, allows the team to acknowledge what worked well, and offers an opportunity to discuss ways to improve processes and procedures.

Participants of a lessons learned session are typically the Project Manager and project team. It may also include the customer and/or external stakeholders as appropriate. Some typical questions to answer include the following:

- In this process or sub process, what did we do well? What could we have changed?
- Did the delivered product meet the specified requirements and goals of the project?
- Was the customer satisfied with the end product?
- Did the project stay within scope?
- Were cost budgets met?
- Was the schedule met?
- Were risks identified and mitigated?
- Were problems or issues resolved timely and adequately?
- Did all of the components of the project management methodology work? If not, which ones did not, and why?
- What could be done to improve the process?

Documenting Lessons Learned Activities

Lessons learned are captured and documented to be housed with other project files and closure documentation. At a minimum, projects should perform a lessons learned review at the end of each major lifecycle phase and at project completion.

Risk Management Roles and Responsibilities

The project manager is responsible for overseeing, monitoring, and assigning all risk management activities, among other project management responsibilities.

The risk owner is responsible for overall execution of the risk management strategy and the corresponding risk management activities, including the following:

- Proposing a strategy for mitigating the assigned risk and getting the strategy approved by the project team and project manager.
- Developing an approach and action plan to execute the management strategy.
- Tracking and reporting on the progress in mitigating the risk.

APPENDIX A. RISK MANAGEMENT PLAN TEMPLATE

This appendix contains an annotated outline of a risk management plan adaptable to individual projects.[4] Use the outline headings for your risk management plan and follow the guidance under the headings:

- *Red italicized text* describes what should be in each section of the risk management plan.
- Black text may be used in your plan as is, or with minor modification.
- Blue underlined text indicates that you "fill in the blank."

[4] Risks should be managed for all projects, regardless of size, and the processes for doing so should be documented. Smaller projects may require a lesser degree of risk management than do larger projects.

Project Name

Risk Management Plan

Version 1.0

DATE

Organizational Unit

Location

UPDATE HISTORY

Version	Date	Nature of Change	Comment
1.0	**Date**	Initial Draft	

TABLE OF CONTENTS

I. Purpose

To introduce the plan, provide a short statement of the purpose, such as the following:

The purpose of this risk management plan is to provide a framework for managing the risks that could hinder the success of Project Name. This risk management plan provides guidelines for identifying, analyzing, documenting, mitigating, and monitoring events that might adversely affect the project. Specifically, this plan provides procedures that

- serve as a basis for identifying, documenting, analyzing, and prioritizing risks associated with the project and for developing management strategies to handle those risks, and
- enable Indian Health Service (IHS), Area Office, and Organization Unit executives and the project team to monitor the health of the project throughout its life cycle.

All information technology projects have risk. Risk management provides a means to identify the potential problems before they occur. Activities addressing these problems are planned and executed, as needed, across the life of the project to mitigate adverse impacts on achieving the project's objectives. To ensure the lowest possible risk in the performance of project efforts, the established goals for this Risk Management Plan are to:

- Identify and analyze risks early and determine their relative importance.
- Provide a tracking system to document, monitor, and update risks systematically.
- Manage risks, if necessary, by handling them appropriately.
- Make timely and appropriate decisions based on risk assessment and monitoring.

II. Background

If the risk management plan is a component of the project management plan, this section may be omitted as it is superfluous. If the risk management plan is a stand-alone document, include a Background Section to place the plan in its context.

A. Organizational Mission

In this section, describe the mission of the organization or operating unit. The mission of the organization or operating unit can probably be extracted from the IHS website and should be edited to focus on that part of the mission that is most relevant to the project's scope and objectives. The description of the mission should be no more than one page.

The Indian Health Service (IHS), an agency within the Department of Health and Human Services, is responsible for providing federal health services to American Indians and Alaska Natives. The provision of health services to members of federally-recognized tribes grew out of the special government-to-government relationship between the federal government and Indian tribes. This relationship, established in 1787, is based on Article I, Section 8 of the Constitution, and has been given form and substance by numerous treaties, laws, Supreme Court decisions, and Executive Orders. The IHS is the principal federal health care provider and health advocate for Indian people and its goal is to assure that comprehensive, culturally acceptable personal and public health services are available and accessible to American Indian and Alaska Native people The IHS currently provides health services to approximately 2 million American Indians and Alaska Natives who belong to more than 566 federally recognized tribes in 35 states.

Describe the mission of the organizational unit that is or will be using the system. This description should put the system in its proper context and should be about one page.

B. Project Name Description

Describe the project's purpose, history, scope, concept of operations, future plans, and life-cycle phase. This should be about one or two pages.

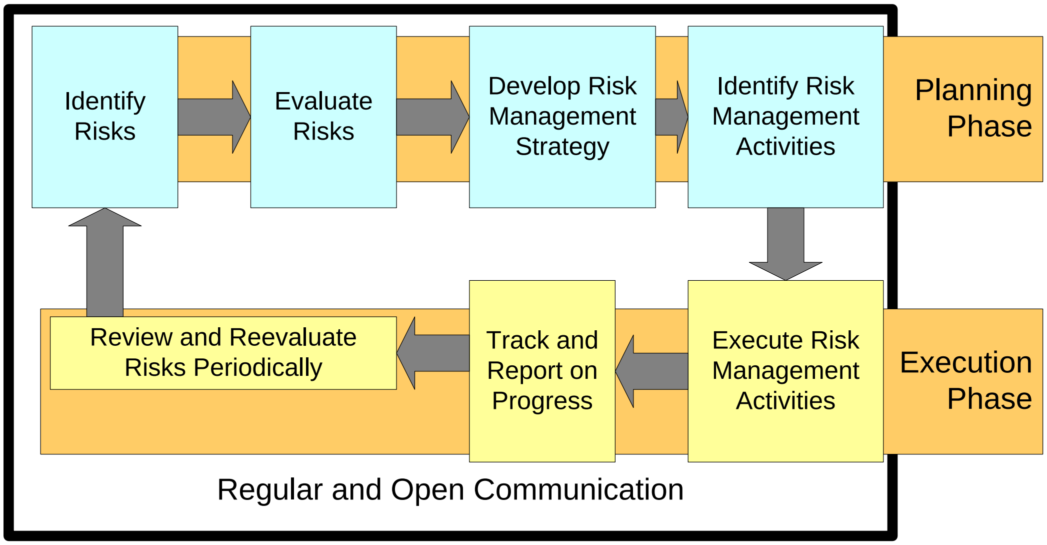
III. The Project Name Risk Management Process

Select a risk management model to be followed. Several are available, including one from the Software Engineering Institute of Carnegie Mellon University.

Describe the model and show it graphically.

Figure 1 depicts the process used to manage risks associated with Project Name. As the figure shows, the process has two phases: a planning phase, and an execution phase. Risk management activities are conducted in an overall atmosphere of regular and open communication within the project team and among stakeholders and users.

Figure 1. Project Name Risk Management Process


Identify Risks
Evaluate Risks
Develop Risk Management Strategy
Identify Risk Management Activities
Planning Phase
Review and Reevaluate Risks Periodically
Track and Report on Progress
Execute Risk Management Activities
Execution Phase
Regular and Open Communication

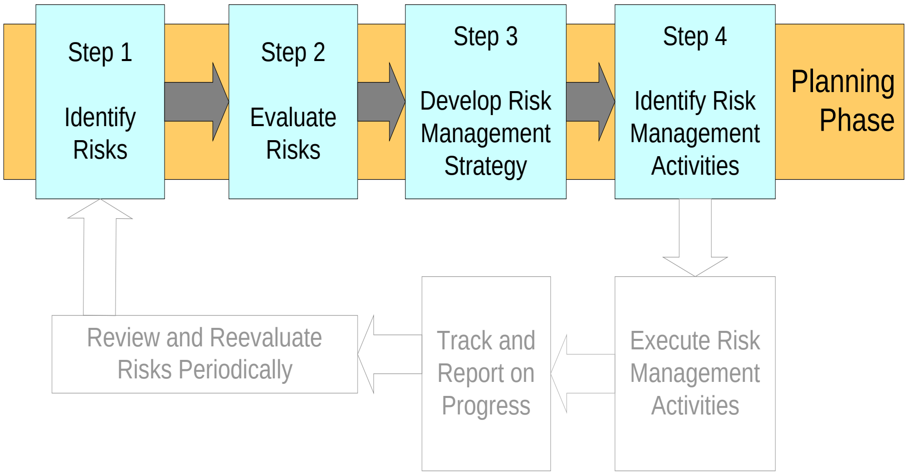
A. Planning Phase

The planning phase of the risk management process has four steps:

- Identify risks
- Evaluate risks
- Develop risk management strategy
- Identify risk management activities

Figure 2 highlights the four steps in the planning phase.

Figure 2. Project Name Risk Management Process—Planning Phase


Step 1
Identify Risks
Step 2
Evaluate Risks
Step 3
Develop Risk Management Strategy
Step 4
Identify Risk Management Activities
Planning Phase
Execute Risk Management Activities
Track and Report on Progress
Review and Reevaluate Risks Periodically

1. Identify Risks

Define risks and describe the process for identifying risks. The following is an example.

Risk identification involves recognizing the critical events that, if they occurred, would prevent the project from achieving its objectives. These events may be related to technological or process uncertainty, cultural resistance to change, lack of progress, failure to achieve critical metrics, or many other factors.

The first step in preparing for risk management is to determine risk sources and categories. Sources are both internal and external to the project. Internal risks are assumed to be capable of being mitigated by the project manager and team. External risks are usually assumed to be outside the control of the project manager and team and will usually need to be elevated to a higher level of management for action or a contingency plan may need to be developed in the event the risk occurs. Due to the dynamic nature of most projects, risk sources can change over the life of the project and will need to be reviewed periodically.

One key factor in recognizing and communicating risk is to state it properly. Best practice is to define specific risks in cause-and-effect statements. State your intent to do so and give a few examples of risk statements that are relevant to the project and its current life-cycle phase. Here are two examples:

> *"If data supporting the legacy system are not accurate and complete, then successful transition to the new system will be jeopardized. "*

> *"If the acquisition process does not include detailed selection criteria and an evaluation plan, then the selection may not be the 'best value' for IHS, and it will not be legally defensible. "*

Describe both continuous and periodic, comprehensive processes for identifying risks. First, introduce the subject.

- Throughout the project's life cycle, risks will be identified in two ways: (1) they will be part of a continuous, ongoing part of project management so that risks are identified and managed as risks arise; and (2) there will be an annual independent, comprehensive assessment of potential risks to assure that potential new risks are fully identified and managed.

Risk sources identify common areas where risks may originate. The following are considered when developing the source lists:

- Changing uncertain requirements
- Change in business need
- Organizational change
- Unprecedented efforts – estimates unavailable
- Infeasible design
- Unavailable technology
- Unrealistic schedule estimates or allocation
- Inadequate staffing, skills, or tool resources
- Cost or funding issues
- Uncertain or inadequate new subcontractor capability
- Uncertain or inadequate new vendor capability
- Other risks outside of the realm of technology.

a. Continuous Risk Identification

Because continuous methods of identifying risk are the first line of defense for a project or program, the project team must maintain an atmosphere of open, candid communication.

Continuous risk identification procedures may vary considerably, from one in which any project team member or stakeholder can formally identify a perceived risk by sending the project manager an e-mail, to procedures involving formal risk identification documentation and a risk committee to evaluate and accept them. Determine the most appropriate level of continuous risk identification for *your project and describe it in a few paragraphs. A smooth-running project in its steady-state phase will require a lesser degree of continuous risk identification than a complex, mission-critical project just beginning the development phase. Use your own judgment to define the best risk identification procedures for your project.*

b. Periodic, Comprehensive Risk Identification

In addition to continuous methods of assessing risk, a comprehensive risk assessment should be a regular part of the project's risk management process. At least annually (and more often if necessary, such as at a significant project milestone), the project team should conduct a comprehensive review of project risks. For example, the review could correlate with the agency budget process and the review and prioritization of agency business cases. Review Appendix B, "Conducting an Open and Comprehensive Risk Review "of this document to determine the appropriate level and schedule for your project. Then describe the chosen approach in a few paragraphs.

2. Evaluate Risks

Introduce risk evaluation.

During the risk evaluation process, the project team will assess all suggested risks, assign each to a risk owner, and enter the risk into the risk tracking process.

a. Risk Rating Method

Describe the method to be used to rate the risks. The following paragraphs describe a two-stage method by first assessing the probability that the risk will occur and the impact of the risk. We then calculate the risk magnitude. Risk Magnitude (=Risk Probability of Occurrence times Risk Impact) is used by the portfolio management tool (PMT) that HHS and IHS use to evaluate the projects for investments that require HHS review and to track those projects. A scoring scheme of High=3, Medium=2, Low=1 is used.

Risk evaluation is an assessment of the magnitude of the identified risks. The Project Name team will measure the risk magnitude by combining estimates of the estimated probability of the risk occurring and the risk's potential impact. The management of risks with a greater magnitude receives more management attention than the management of risks with lesser levels of magnitude.

Table 1 provides the ratings and guidelines for the estimated probability that the risk situation will occur. Table 2 provides the ratings and guidelines for estimating the degree of impact on the project if the risk is not mitigated.

Table 1. Probability of Occurrence

Probability	Rating	Guideline
Low	1	Below 30% probability of occurrence
Medium	2	Between 30% and 70% probability of occurrence
High	3	Greater than 70% probability of occurrence

Table 2. Degree of Impact

Impact	Rating	Guideline
Low	1	Will have minor impact on system development or operation
Medium	2	Will likely cause delay in one or more functions required to develop or operate the system
High	3	Will likely cause a significant delay and/or stoppage in system development or operation

The magnitude for each risk is then calculated by multiplying its rating for degree of impact by its probability of occurrence rating:

Risk Magnitude = Probability × *Impact.*

Table 3 shows the guidelines used to determine the risk magnitude for each attribute.

Table 3. Risk Magnitude

Magnitude	Rating	Guideline
Low	1 or 2	Low likelihood of the risk moderately impacting one or more factors.
Medium	3 or 4	Medium likelihood of the risk moderately impacting one or more factors.
High	6 or 9	High likelihood of the risk severely affecting one or more factors. May have a high potential of causing program stoppage.

b. Actions for Different Risk Magnitude Ratings

Different risk magnitude ratings may require the project manager and the risk owner to apply different risk management actions, such as the following:

- Notifying senior management of project risk. A risk with a probability of occurrence of High = 3 and potential impact on the program of High = 3, resulting in a risk magnitude of High = 9 might be required to be reported as soon as possible to senior management officials (the project sponsor and the IHS Chief Information Officer (CIO), for example).

- Assigning a risk owner. A risk with a medium or high magnitude (risk magnitude = 3, 4, 6, or 9) might have a risk owner assigned and have risk management activities developed for it. Risks with a lower risk magnitude might be handled in a less intensive manner.

- Developing a risk management strategy and plan. A risk with a low magnitude (risk magnitude = 1 or 2) might be tracked by the project manager but not have an assigned risk owner or risk management activities.

Appropriate risk management action depends on risk magnitude, the nature and complexity of the project itself, and good management judgment.

Determine the appropriate level of risk tracking for your project and describe it in a few paragraphs.

3. Develop Risk Management Strategy

The most appropriate strategy for managing each risk should be determined. If a negative risk can be avoided (e.g., changing the project plan), if it is transferred (e.g., though the use of a firm fixed- price contract), or if it is accepted (e.g., there is no other suitable response strategy), it need no longer be part of the on-going risk management strategy, although it should be identified and the action taken on documented. The remaining risk management strategy for a negative risk should be to develop a risk management strategy, which is what you do to try to keep the risk from occurring in the first place.

For a positive risk (i.e., an opportunity), the risk management strategy may include exploiting it by insuring that the opportunity will definitely happen; sharing or transferring it to another organization that can best take advantage of it; or enhancing it or increasing the probability of the opportunity occurring.

Regardless of whether the risk is positive or negative, if it is a risk that is being managed and is of medium or of high magnitude, you should also develop a risk response or contingency plan, which is what you plan to do if the risk occurs. The risk management strategy is expressed in a short statement that describes the approach to managing the risk. For a risk with a high magnitude, a specific risk owner may be assigned to manage the risk and its management activities. For negative risks that cannot be mitigated or which are too expensive to mitigate, a risk response or contingency plan should be developed.

Give one or two examples that are relevant to your project. An example follows:

It is the responsibility of the risk owner to develop an appropriate risk management or risk management strategy and to get it approved by the Project Name team.

The risk management strategy is a short statement that describes the approach to managing the risk. For example, the statement below describes a mitigation strategy for a system interface risk:

> *"The organization will acquire an independent validation and verification (IV&V) contractor to assist with developing interface test requirements and an integrated test plan, and it will perform interface testing before acceptance."*

The statement below is an example of a mitigation strategy for the risk of declining system effectiveness from the perspective of users:

> *"Continuous assessment of program usability and effectiveness will be maintained though open communication and regular user group meetings. Users will participate in annual program risk assessment exercises. "*

Management strategies may be even more concise. Here's an example of a security risk mitigation statement:

> *"The project manager will implement the security protocols provided by IHS and NIST. "*

There are other approaches to risk management other than mitigation that may be appropriate. Any of these approaches could be a risk management strategy that should be documented in the risk management plan:

- Changing the project plan to eliminate the risk altogether
- Transferring the risk impact to a third party
- Accepting that there is no cost-effective approach to mitigation and that contingency planning will be the best way to manage the risk. Active acceptance may involve the creation of contingency plans and passive acceptance may leave actions to be determined as needed. A decision to accept a risk must be communicated to stakeholders.

4. Identify Risk Management Activities

Describe how you plan to have risk management actions developed by the risk owner (or whomever else might be assigned responsibility for developing the plans), and how risk management activities are approved, tracked and reported.

A variety of approaches are possible depending on the complexity and life-cycle phase of the project and the complexity of the risk management strategy. For example, for simple risk management strategies, a list of actions with due dates and responsibilities may suffice. Or, for complex or high-magnitude risks, a detailed plan for risk management might be needed. Using Microsoft Project as a tool to help manage the risk management activities may be appropriate.

Determine the best approach for your project and describe it in a few paragraphs. Say something like the following.

Once the risk management strategy is approved by the project team, the risk owner will develop an approach and propose actions to execute the risk management strategy. The proposed actions are defined in a work plan, unless a more detailed approach is directed by the project manager.

With the help of the project manager, appropriate members of the team and others as necessary, the risk management actions will be assigned to specific individuals and formalized.

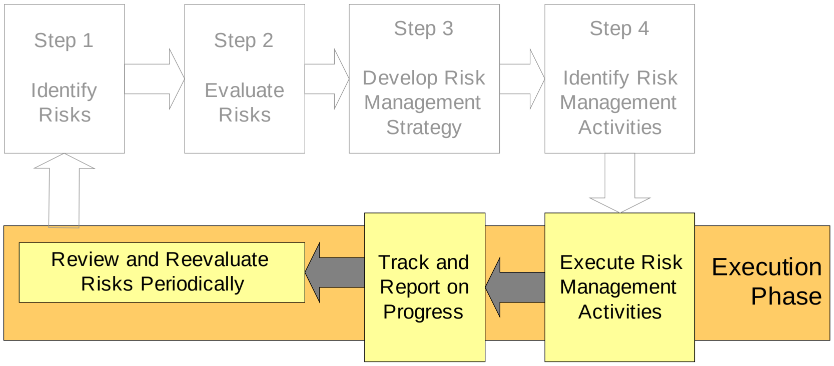
The risk owner tracks and reports on progress toward risk management at predetermined risk review sessions conducted by the project team—at least monthly.

B. Execution Phase

Figure 3 highlights the execution phase of the risk management process. This phase has three steps:

- Execute risk management activities
- Track and report on progress
- Review and reevaluate risks periodically

Figure 3. Project Name Risk Management Process—Execution Phase


Step 1
Identify Risks
Step 2
Evaluate Risks
Step 3
Develop Risk Management Strategy
Step 4
Identify Risk Management Activities
Review and Reevaluate Risks Periodically
Track and Report on Progress
Execute Risk Management Activities
Execution Phase

1. Execute Risk Management Activities

Describe responsibilities for execution of the risk management activities in a few paragraphs. Say something like the following.

Those responsible for executing the risk management activities will execute them in accordance with the plans managed by the risk owners.

The risk owner maintains responsibility for overall execution of the risk management strategy and the corresponding risk management activities.

2. Track and Report on Progress

Describe how information on risks and risk management planned activities will be tracked. Begin by stating something like the following.

Performance and progress on mitigating the risks are tracked against the risk management activities. Progress against the risk management plan is available for review by the project manager and designated members of the project team at any time.

Then, describe the reporting schedules and venues for reporting by the risk owners. Many reporting options are possible depending on the nature of the project and the severity of the risk. Low-severity risks on stable operating systems may be reviewed by the project team at a regularly scheduled meeting at least once each quarter. For complex or high-magnitude risks or for risks associated with a large, complex, and mission-critical project, more frequent reporting is warranted. In some cases, it may be appropriate to hold a weekly or monthly ad hoc project risk meeting that is attended by stakeholders and senior managers, as well as team members.

In all situations, information on risks, their risk management strategies, risk management activities, and progress toward mitigation should be available to appropriate staff and managers.

Progress toward mitigating risks will be reported annually to senior Area Office/Organization Unit and IHS management and to OMB through the CPIC process and the OMB Exhibit 300.

If you plan to report high risks to senior management as soon as they are identified, as discussed in the Evaluate Risks section (III. A. 2. b), include this reporting requirement here as well. The following is an example.

The IHS CIO will be notified and briefed whenever a high-magnitude risk is identified.

3. Review and Reevaluate Risks Periodically

Describe plans for periodic review and reevaluation of risks. It should be done at least annually but should also be performed at significant project milestones, such as after selection of a system integrator or at completion of end-to-end testing. Describe what is appropriate for your project. The following is an example.

The project team, led by the project manager, will assist with a periodic comprehensive review of the risk posture of the Investments. This review will take place at least once each year in preparation for the annual business case review and prioritization by the IHS Information Technology Investment Review Board (ITIRB).

During the reevaluation process, it may be determined that some risks that were identified in past evaluations, or as part of the ongoing risk identification process, have been successfully mitigated. These risks will still be listed on the risk inventory with an annotation that no action is necessary, the risk has been successfully mitigated. This will demonstrate that the risk was identified and managed at some time as part of the risk identification and assessment process.

IV. Risk Management Roles and Responsibilities

Describe the risk management roles and responsibilities for your project. Include at least the project manager and the risk owner. Review and cite the roles and responsibilities sections for the CPIC program contained in Capital Planning and Investment Control Policy and Guidelines *issued by the Office of the CIO. Say something like the following.*

The project manager and the risk owner have specific risk management responsibilities for project risk management.

A. Project Name Project Manager

The project manager is responsible for overseeing, monitoring, and assigning all risk management activities.

The project manager will schedule a periodic independent review of program risks at least once each year. This review will cover the perspectives of all program stakeholders. It will result in identified risks, risk ratings, and suggested risk management strategies.

B. Risk Owner

The risk owner has the following responsibilities:

- Propose a strategy for mitigating the assigned risk and get the strategy approved by the team and project manager

- Develop an approach and action plan to execute the risk management strategy

- With the help of the project manager, assign responsibility for completion of the action plan steps

- Track and report on progress in mitigating the risk

APPROVALS:

Jonas Salk
Project Investment Manger

Date

Howard Hays
Chief Information Officer (Acting)

Date

Samuel Mudd
Project Sponsor

Date

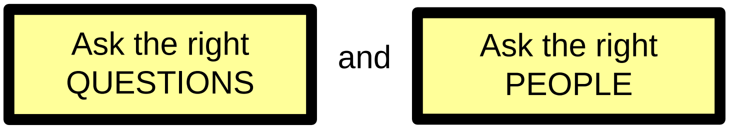
APPENDIX B. CONDUCTING AN OPEN AND COMPREHENSIVE RISK REVIEW

Risk management includes assessment of risk, development and execution of risk management strategies, and monitoring of progress. This appendix provides guidance on how to conduct a risk assessment.

Risk assessment involves identifying and understanding the potential risks during project development and implementation: the events that, if they occurred, would prevent the project from achieving its cost, schedule, or performance objectives. These events may be related to technological or process uncertainty, cultural resistance to change, lack of progress, failure to achieve critical metrics, or many other factors.

One effective way of assessing risk is through a periodic, open and comprehensive risk review.[5] The risk review team normally consists of a leader and one or two team members. The team convenes representatives from the project staff, users, and stakeholders in an environment of open communication. The risk review must be comprehensive so that the full spectrum of risks from all sources is considered. During a risk review, the risk assessment team must ask the right questions and ask the right people, as shown in Figure B-1.

Figure B-1. Two Elements of Effective Risk Assessment



Ask the right QUESTIONS

and

Ask the right PEOPLE

Ask the Right Questions

Risks that are managed are minimized. Understanding and communicating project risks help manage the expectations of senior management and other stakeholders. One such stakeholder, OMB, may ask for the formal risk management plan and annual reporting of project risks and risk management progress before approving requested project funding.

OMB's risk management reporting requirements for large projects are useful for managing risk in projects of all sizes because they contain a broad, comprehensive set of risk categories that are useful to project managers as a starting point for defining their project risks.

[5] Two important ways of identifying risk are continuous risk identification, which requires an open and honest exchange of ideas as part of daily project management, and comprehensive risk identification, which entails a periodic assessment of risk on a project-wide basis. For additional information on these types of risk identification, see Appendix A, Section III.A.1, Identify Risks.

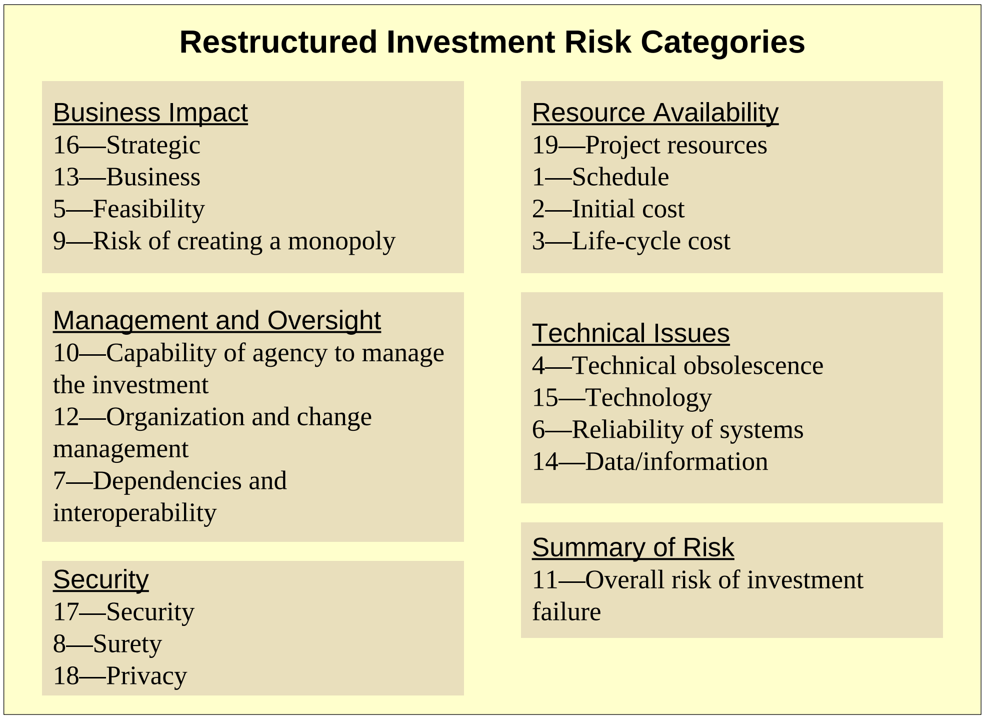
OMB has identified 19 risk categories, presented in Figure B-2, that provide a minimum set of risk areas to be considered by the project risk assessment team.

Figure B-2. OMB's 19 Risk Categories

Risk Categories for All Investments	Risk Categories for IT Investments
1) Schedule	12) Organizational and change management
2) Initial cost	13) Business
3) Life-cycle cost	14) Data/information
4) Technical obsolescence	15) Technology
5) Feasibility	16) Strategic
6) Reliability of systems	17) Security
7) Dependencies and interoperability	18) Privacy
8) Surety (asset protections)	19) Project resources
9) Risk of creating a monopoly	
10) Capability of agency to manage the investment	
11) Overall risk of investment failure	

The figure separates the risks into two categories: (1) those for all investments and (2) those for IT investments. There are similarities between those in the first set of risk categories and those in the second. It is helpful to consider the risks grouped according to their overall management-related area. Reordering the risk categories into related risk areas, as shown in Figure B-3, makes them more user friendly and more meaningful to technical personnel, functional users, and senior management.

Figure B-3. Restructured OMB Risk Categories



Restructured Investment Risk Categories

Business Impact
16—Strategic
13—Business
5—Feasibility
9—Risk of creating a monopoly

Management and Oversight
10—Capability of agency to manage the investment
12—Organization and change management
7—Dependencies and interoperability

Security
17—Security
8—Surety
18—Privacy

Resource Availability
19—Project resources
1—Schedule
2—Initial cost
3—Life-cycle cost

Technical Issues
4—Technical obsolescence
15—Technology
6—Reliability of systems
14—Data/information

Summary of Risk
11—Overall risk of investment failure

The order of assessing these risks doesn't matter. However, it improves the ability of the risk assessment team to identify risks if the assessment starts with those areas that are broadest in scope. The risk assessment leader should start the assessment with Business Impact; the highest level, least technical of the risk areas. Next the risk assessment leader should address the other areas according to Resource Availability, Management and Oversight, Technical Issues, and Security, the most narrow and specialized area. The risk assessment leader should address the Summary of Risk last. Table B-1 lists the order in which the risks should be addressed and provides some examples of topics that may be considered while assessing risk in each risk category.

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Business Impact	16—Strategic	Risk associated with strategic/government-wide goals top management support and communication, consistency with strategic plans, high-level visibility with outside stakeholders such as OMB or Congress, and other political impacts. Risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them. Risk that strategic goals and objectives, including PMA goals or HHS priorities, may change. Risk that the objectives of the project are not clearly linked to program needs, to the agency's overall strategies, and to government-wide policies and standards. Risk that the initiative 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).	• Does this project support a government wide initiative? • Does this project support the strategic goal(s) of HHS or of the OPDIVs? • Have stakeholders (e.g., OPDIVs) been engaged? Do stakeholders have buy-in with scope and requirements?
	13—Business	Risk associated with the validly of the business case for the project, the completeness and validly of the specified functional requirements, and the need for reengineering subject business processes. Risk that the business goals of the program or initiative will not be achieved. Risk that the program effectiveness targeted by the project will not be achieved.	• Is the business need and project scope well-defined? • Have the planned improvements/benefits to business operations or customer results been documented? • Have operational performance measures been identified and signed-off by the sponsor and (OPDIVs) major stakeholders? • Has an Operational Analysis been performed at least annually? • Have any shortcomings been identified?
	5—Feasibility	Risk associated with the feasibility of the requirements from a technical and performance point of view and the organization's familiarity with the project life-cycle method used within the organization or as implemented by others. Risk of insufficient ability to successfully develop and implement the project within defined technical, scope, cost, and schedule parameters to successfully meet the performance goals.	• Is the proposed technology involved feasible? • Has an alternatives analysis been performed, is it less than 3 years old? Does/did the alternatives analysis examine use of other technologies (e.g., different COTS products and/or different hosting solutions: Cloud Computing/private cloud)? • Is the proposed solution feasible? • Is the solution as simple as possible?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Business Impact	9—Risk of creating a monopoly	Risk associated with the over-reliance on a particular vendor or on proprietary or specialty software that would limit project expansion or flexibility.	• Does the technology/vendor selected trigger a risk that the Department/OPDIV will be locked in to a specific set of vendors and their products?
Resource Availability	19—Project resources	Risk associated with the stability and adequacy of project staff and project budget for today and the future. Include resources that might be available from contractors. Risk that the availability of people, funds, schedule, and tools that are the necessary ingredients for successfully implementing the project will be inadequate (if any are inadequate, including the qualifications of the people, there is risk). Risk that appropriate training will not be available in a timely fashion.	• Do the COTS vendors have and established reputation of delivering quality product on time? • Are the contractors qualified for this type of work; do they have an established track record? • Are requirements/scope, cost and schedule well defined? • Are necessary algorithms or work flows well understood? • Do the contract vehicles provide cost controls; are they appropriate to the product and/or service to be provided? • Has the project management team worked with the business owners/stakeholders to identify capabilities or components that might need to be reschedule or delayed in the event that budget cuts affect the ability to authorize and execute tasks as planned?
	1—Schedule	Risk associated with the stability, reality, and validity of the time estimated and allocated for the development, deployment, and operation of the system. Include the cost or impact of not meeting the schedule. Two risk areas bearing on schedule risk are (1) the risk that the schedule estimates and objectives are not realistic and (2) the risk that program execution will fall short of the schedule objectives.	• Does the project have an Integrated Master Schedule? • Is there a high level of confidence in the schedule for the project? • Does the schedule address all of the EPLC documentation in addition to the functional deliverables? • If processes and procedures are being affected is delivering training and developing the related documentation included in the schedule?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Resource Availability	2—Initial cost	Risk associated with the adequacy, completeness, accuracy, and validity of the initial funding estimates, the supporting information that justifies those initial funding estimates, and their relationship to longer term funding needs.	• Is there a high level of confidence in the estimates for the project? • Is the project scope sufficiently defined to identify size/scale/complexity of the project effort? • Are the estimates based on two or more reliable estimating techniques? • Have management and oversight requirements, such as workflow/status reporting, identified? • Are the requirements well understood and well developed? • Are security requirements well established? • Do security requirements include audit logging and regular analysis of audit logs? • In addition to the functionality and security requirements, have all of the "ility" requirements been identified (i.e., reliability, availability, maintainability, usability, supportability, etc.)?
	3—Life-cycle cost	Risk associated with the adequacy, completeness, accuracy, and validity of life-cycle cost estimates, the supporting information that justifies those life-cycle funding estimates, and the likely stability of longer term availability of funds. This includes the impact of errors in the cost estimating technique(s) used (given that the technical requirements were properly defined). Lifecycle costs include planning, development, operations, and retirement costs.	• If this project is going to be followed by additional functionality • Is there a good understanding of the projects/enhancements that are needed? • Has the additional functionality been considered in the design? • Is the system solution designed to be maintainable • Is the design and acquisition structured so the solution is not a proprietary solution that can only be supported by one vendor/competitor? • Are training and maintenance costs considered in the life cycle cost analysis? • Will the planned solution/system be supportable, and maintainable? • What is the plan for maintaining the system once it is deployed? • Is there funding to maintain this system?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Management and Oversight	10—Capability of agency to manage the investment	Risk associated with the experience of the project manager and staff' in the development or operation of systems with similar complexity and/or size, the application domain, and the functional business processes involved. 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 the development or operation of projects of similar complexity and/or size, the application domain, and the functional business processes involved. Also relates to the degree to which program plans and strategies exist and are realistic and consistent.	• Does the project have a PM with experience in this type and/or size of project? • Does the PM have certification and/or appropriate training? • Does the project have team members with appropriate experience to manage, track progress and ensure quality deliverables (e.g., PM, EPLC or technical expertise appropriate to type of project)? • Are good project management, acquisition management, requirements management, etc., controls in place? • Are there adequate tools for planning and managing the project?
	12—Organization and change management	Risk associated with the willingness and ability of the organization/agency to accept the cultural, process, and procedural changes required by the project. Include the existence or adequacy of the change management plan, communications plan, and user training plan. Risk associated with bypassing, lack of use, improper use, or adherence to new systems and processes due to organizational structure and culture; inadequate training.	• Is organizational change required? • Is reengineering/ reorganizing of business processes or workflows required? • Is there adequate backing by sponsors and key stakeholders? • Are planned changes well communicated? • Is training for new system as well as new processes planned?
	7—Dependencies and interoperability	Risk associated with the dependence of the project on data from other systems and processes (existing and planned) (existing or in development) within the Agency and across the Federal Government (e.g. technical interfaces, schedule dependencies). Risk associated with the requirement for the project to operate in concert with other programs. Include related schedule and funding concerns. Risk is increased if the success of a project is directly linked to the success/ implementation or on-going maintenance of other systems.	• Are the internal and external interfaces identified and well understood? • Are dependencies and interoperability requirements well defined? • Is there an Interface Control Document (ICD) for each interface/connection between communicating systems that specifies the data, format, communications protocol, periodicity, expected volumes, etc? • Are there signed Service Level Agreements (SLAs) or Memoranda of Understanding (MOUs) that address reliability, availability, security data integrity, etc?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Technical Issues	4—Technical obsolescence	Risk associated with the likelihood of the technology becoming obsolete because of changing technology or requirements. Include technology support from the existing supplier and ability of in-house staff to manage support. 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.	• Is the technology "aging" and in danger of obsolescence? • Is there a danger that the development language or other COTS products are so old that it would be difficult to get and/or maintain a qualified team for the project as well as the anticipated life cycle of the system? • If this project provides an upgrade or replacement to an existing system, are there plans for retirement and disposition of the current system/solution?
	15—Technology	Risk associated with the existing or chosen software, hardware, and network reliability, maintainability, and security. Include technology documentation, testability, and appropriateness for the functional need in the existing or future environment. Risk associated with immaturity of commercially available technology. 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.	• Is the technology bleeding edge? • Is the technology considered mature enough to be reliable? • Are there multiple vendors that are able to provide the support/services needed on this technology? • Do the team members have appropriate expertise? • Is the technology mature enough?
	6—Reliability of systems	Risk associated with the defined response time and throughput requirements as needed and expected. Include system contingency plans, continuity of operations plans, disaster recovery plans and tests of those plans. Risk of inability of the system to provide planned and desired functionality.	• Does the proposed solution provide a sufficiently robust and/or redundant solution that system and data availability requirements are met? • Are physical and IT security measures sufficient to ensure the security of the IT system and the integrity of the data?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Technical Issues	14—Data/ information	Risk associated with the clarity, completeness, validity, sources, and feasibility of data requirements. Include data interface and data conversion complexities. Include data collection, storage, integrity, and availability. Risk associated with the loss/misuse of data or information, risk of increased burden on citizens and businesses due to data collection requirements if the associated business processes or the project require access to data from other sources (federal, state and/or local agencies).	• Has a Privacy Impact Assessment (PIA) been performed or revisited in the last 2 years? • If any Personally Identifiable Information (PII) is collected, has the need for that information been established? • Have the requirements for the analysis, reporting and or other use of this data been well established? • If multiple sources of PII are combined, has that been announced in a System of Records Notice (SORN)? • Are processes and security controls in place to ensure authorized users have a need for access to the system/data and that the users are granted only the (role-based) access they need? • Are there controls in place to prevent unauthorized access/viewing, combination, and/or analysis of the PII? • Are data being supplied by trusted sources? • Is there a way to check the integrity and/or validity of the data? Are interfaces and data feeds/pulls well defined? • Is there a data migration plan for transition of data from legacy to replacement system(s)? • Is there an approved records management plan?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Security	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 Risk associated with the validity and effectiveness of the organization security plan, the plan's compliance with NIST requirements, associated plans to certify and accredit the IT system prior to implementation, and the organization's ability to implement the plan. [Note: This risk category must include in the risk description the level of risk (high, medium, or low) and what aspect of security determines the level of risk, e.g. need for confidentiality of information associated with the project/system, availability of the information or system, or reliability of the information or system.]	• Are physical security controls in place? • Are adequate personnel checks in place? • Is there role-based access control and separation of responsibilities to ensure adequate information security controls are in place? • Do the COTS products provide tools that support FISMA requirements? • Does/will the system have current Certification and Accreditation (C&A) and/or Authority To Operate (ATO)? • Are interfacing systems subject to security checks and access controls?
	8—Surety (asset protection)	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. Risk associated with the nature, value, and security of physical assets (government or contractor owned) and the contingency plans to protect the project in the event of asset loss or failure.	• Are there adequate checks/controls to ensure data integrity and appropriate level of access control? • Are the selected systems/technologies reliable? • Are processes in place to ensure transfer of data is reliable, and to ensure that transmitted/transferred data reaches only the intended recipient system(s)?
	18—Privacy	Risk associated with the vulnerability of the collection, use, storage, transmission, and disposal of personally identifiable or proprietary information. Risk associated with the compliance with the Privacy Act and the privacy impact assessment. Include the effectiveness and cost of the project's documented standards for submission and use of personal information.	• Has a Privacy Impact Assessment (PIA) been performed? • If this is a project related to a legacy system, has the PIA been revisited in the last 2 years? • Does/will the system contain Personally Identifiable Information (PII) of the general public or of employees?

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations	Sample Questions
Summary of Risk	11—Overall risk of investment failure	Risk associated with any risks, including other risks not already discussed, that have the greatest potential for causing system failure or that have a negative impact resulting from the occurrence of one or more identified or unidentified risks, leading to catastrophic results for the project. It refers to the aggregation of identified risks associated with this initiative and the likelihood (probability and impact) that one or more occurrences of risk will cause this initiative to fail. It also includes the risk that unidentified activities occur that lead to the project becoming obsolete. Include the effectiveness and use of the risk management plan.	• Is there a business need for this project? • Does the product/system support the business goals and objectives? Is this project a business priority? • Has the sponsor/business owner been identified? • Does the sponsor/business owner his/her recognize role and responsibilities with the project? • Is there sufficient support for completing this effort and backing to get allocation of funds? • Are there political issues that might affect the direction and/or priority of this effort? • Are the requirements well understood and well managed? • Is the design well documented? • Is the test plan well-documented? • Do the tests map to the requirements? • Is there a sound implementation plan? • Is there a sound training plan? • Are there adequate tools for executing the project, for requirements analysis and management, design, development, test, implementation/deployment? • Do team members have adequate training to use the tools and perform their job/role? • Are roles and responsibilities within the project team clear? • Is there a training plan? • Do key individuals have backup/shadow personnel? • Is there any succession planning?

Ask the Right People

WHOM TO ASK

Whose opinion of project risk is the best to solicit? The answer is anyone who has a stake in the project's success. No one group of people is best for every project or every life-cycle phase of a single project. The appropriate people include individuals selected from this list:

- Project or investment management
- Project staff
- Organization or operating unit security officer
- Organization or operating unit and/or IHS chief enterprise architect
- Agency support staff such as the budget officer and the contracting officer
- Contractor management
- Contractor staff
- Users or potential users
- Senior functional management and senior technical management
- Other members of the Integrated Project Team (IPT)
- Other stakeholders that have an interest in the success of the project and a perspective about risk.

Do not exclude people because they are not supporters of the project or because you think you already understand their opinions. These may be the most important people to include. Getting potential real or perceived risks out in the open early is often the best way to manage or mitigate them.

It is best to gather opinions of risk in an open forum so all players can hear and learn from the ideas of others. For this reason, a facilitated workshop is recommended.

DON'T ATTEMPT TOO MUCH

While a group is gathered to identify and evaluate project risk, it may be tempting to try to cover too much ground—for example, to also develop risk management strategies and discuss risk management action steps. These are best postponed until a later meeting or until the risk owner is ready to discuss them. A more limited agenda works best. Suggestions for an agenda are listed below:

- Describe the purpose of risk management and the risk management model. Introduce the risk categories.
- Address each risk category. You may not have a risk in every category; however, every category should be reviewed. State each risk as a cause-and-effect statement.
- When all risks have been identified, consider them in their entirety. Then evaluate each risk—one at a time—for its potential impact on the project and the likelihood of occurrence as described in your risk management plan.

If time permits, consider risk management strategies for the most serious risks. If appropriate, assign risks to risk owners as described in the risk management plan.

A sample risk inventory and assessment, the results of conducting an open and comprehensive risk review, is presented in Appendix C.

APPENDIX C. SAMPLE RISK INVENTORY AND ASSESSMENT

This Appendix provides a sample risk inventory and assessment.

When entered into the HHS project and Portfolio Management Tool, Oracle Primavera ProSight, a unique identifier for each risk identifier will be assigned by the tool

Within a risk category, there can be more than one risk (see risk category *4) Technical Obsolescence*, for example).

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment
As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Schedule data	10 Jan 2013	1) Schedule	If the project manager does not have the appropriate information to track actual progress against planned milestones, then the project may fall behind schedule.	Low	Low	1	None required. Risk is minimal.	Schedule issues involving system modification are managed through regular weekly team meetings.	10 Jan 2013: Risk initially identified.
Initial cost data	10 Jan 2013	2) Initial Costs	If the initial cost estimate is not accurate, then the lifecycle costs and future estimates will not be accurate.	Low	Low	1	None required. Risk is minimal.	GSA purchase.	10 Jan 2013: Risk initially identified. 16 Jan 2013: Purchase completed.
Life-cycle cost data	10 Jan 2013	3) Life-cycle Costs	If life-cycle costs are estimated incorrectly, then project may not be completed within the specified budget.	Low	Low	1	None required. Risk is minimal.	COTS product; GSA purchase. System is primarily in the steady-state phase of its life cycle and DME costs are relatively low. Those requesting enhancements participate in funding justifications.	10 Jan 2013: Risk initially identified.
Maintenance costs	10 Jan 2013	4) Technical obsolescence	If the Investment relies on technology that is not open or widely supported, then the maintenance may become cost-prohibitive.	Low	Low	1	None required. Risk is minimal.	Auto-refresh with contractor.	10 Jan 2013: Risk initially identified.
Oracle migration	10 Jan 2013	4) Technical obsolescence	If the standard Oracle migration path is not followed, the system could become technologically obsolete, more expensive to maintain, and/or lose functionality.	Low	Low	1	None required	The Oracle contractor attends weekly ITDS team meetings and reports on Oracle technology change issues. Project personnel have extensive experience with the Oracle products.	10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment
As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Design complexity	10 Jan 2013	5) Feasibility	If the implementation of the design is difficult or impossible to test, the project may be accepted when it does not meet user-defined functional requirements.	Low	Low	1	None required. Risk is minimal.	COTS product; GSA purchase.	10 Jan 2013: Risk initially identified.
System restoration	10 Jan 2013	6) Reliability of systems	If the staff has limited expertise with technology, then the ability to quickly restore and repair systems could be impacted.	Low	Low	1	None required. Risk is minimal.	COTS product; meets business need.	10 Jan 2013: Risk initially identified.
Software / hardware reliability	10 Jan 2013	6) Reliability of systems	If the software places unexpected stress on the hardware and other infrastructure, the system may fail.	Low	Low	1	None required	The software, hardware, and infrastructure have proven their ability to support the system. The system has a continuity of operations plan and a disaster recovery site. System reliability has not been an issue.	10 Jan 2013: Risk initially identified.
Shared system	10 Jan 2013	6) Reliability of systems	If a change is made in the hardware or software to accommodate other work without evaluating its impact on all systems, ITDS may fail.	Medium	Low	2	None required	System is primarily in the steady-state phase of its life cycle and hardware and software changes are coordinated among affected parties. Risk is continuous and will be regularly monitored.	10 Jan 2013: Risk initially identified.
Planned interoperation	10 Jan 2013	7) Dependencies/ interoperability	If the internal and external system dependencies and ability to interoperate are not adequately planned for, the system may not be as effective and costs could increase.	Low	Low	1	None required. Risk is minimal.	No dependencies and interoperability risks have been identified. ITDS is a stand-alone application.	10 Jan 2013: Risk initially identified.
Asset protection	10 Jan 2013	8) Surety	If the fixed, intellectual, and human assets are not protected adequately from harm, then the investment may be impacted.	Low	Low	1	None required. Risk is minimal.		10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Monopoly avoidance	10 Jan 2013	9) Risk of Creating a Monopoly	If the investment relies on one or two vendors, then the risk of creating a monopoly increasing and innovation may be stifled.	Low	Low	1	None required. Risk is minimal.	IHS uses full and open competition. Some contracts, by the nature of the technology, are dependent on a particular company – i.e., Cisco Routers, MCI backbone.	10 Jan 2013: Risk initially identified.
Project management skills	10 Jan 2013	10) Capability of Agency to Manage the Investment	If project managers are not sufficiently skilled in project management, software development, software management, or the development process, the project could fail.	Medium	Medium	4	Laura Lee Hope 301-443-1234	Project manager is an experienced federal manager. Project manager is taking project management training and will be certified by December 2013.	10 Jan 2013: Risk initially identified. 14 Feb 2013: Project manager is taking project management courses as scheduled. Expected certification by December 2013. Continue monitoring.
Project monitoring	10 Jan 2013	11) Overall project failure	If Inadequate attention is paid to monitoring cost, schedule, and performance goals, then the investment may be impacted.	Low	High	3	Capt. Mark Twain will monitor EVM variances monthly.	COTS product; planned use similar to previous use	10 Jan 2013: Risk initially identified. 14 Feb 2013: Project schedule variance i-3.37% Project cost variance is -4.05%. Continue monitoring.
Stakeholder support	10 Jan 2013	12) Org/Change Management	If the stakeholders do not support the investment or major organizational changes occur, the investment may not meet performance goals.	Low	Low	1	None required. Risk is minimal.	The program conducts regular performance reviews with management and key users.	10 Jan 2013: Risk initially identified.
Sponsor support	10 Jan 2013	13) Business	If the investment does not have active project sponsor support, then resources, funding, schedule, and management support could be impacted.	Low	Low	1	None required. Risk is minimal.	The investment manager meets regularly with key business managers and the CIO's office.	10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment
As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Poorly defined field names	10 Jan 2013	13) Business	If the end user is unable to easily understand the field name semantics, data may become inconsistent.	Medium	Medium	4	Flossie Bobbsie 505-248-1234	Critical data elements for ITDS are being defined and will be converted into Common Data Elements (CDEs). The CDEs created for ITDS will be added to the Infrared Terosis Standards Repository (ITSR) as they are finalized. The estimated completion date is December 29, 2013. CDEs from other IHS context areas will be reused where appropriate. Meetings will be held with key staff members for IHS entities that manage protocols to develop a core set of CDEs that will accommodate the processing of protocols and related documents. The estimated completion date is December 29, 2013.	10 Jan 2013: Risk initially identified. 14 Feb 2013: First meeting is scheduled for 1 April 2013.
Data loss	10 Jan 2013	14) Data/Info	If the investment incurs data loss, then dependent systems could be compromised.	Low	Low	1	None required. Risk is minimal.	Regularly monitoring of data.	10 Jan 2013: Risk initially identified.
Data requirements	10 Jan 2013	14) Data/Info	If data requirements are unclear to data suppliers, data collected may be inconsistent, incomplete, and inaccurate. (See risk “Poorly Defined Field Names” 13—Business.)	Medium	Medium	4	Flossie Bobbsie 505-248-1234	Train data suppliers. When the severity of adverse events for Vioxx was identified, 26 prevention trials were underway. It took four staff members more than a week to gather the necessary data to expeditiously notify investigators and participants, stop the trials, and stop the drug shipments.	10 Jan 2013: Risk initially identified. 14 Feb 2013. Orientation meeting scheduled for data suppliers on 1 April 2013. Continue monitoring.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Bleeding edge	10 Jan 2013	15) Technology	If the investment is developed with new performance-enhancing technology, then the investment may incur additional training, testing, and implementation activities.	Low	Low	1	None required. Risk is minimal.	Tested and commonly used applications/COTS products used to meet requirements where possible Staff has access to training in new technology. The investment has built the risk of any new technology into cost and schedule projections.	10 Jan 2013: Risk initially identified.
Strategic direction	10 Jan 2013	16) Strategic	If changes in HHS IT goals or federal health architecture mandates occur, the investment will be impacted.	Low	Low	1	None required. Risk is minimal.	The investment manager continually monitors upcoming HHS and HHS IT initiatives for impact on program.	10 Jan 2013: Risk initially identified.
Data response	10 Jan 2013	16) Strategic	If ITDS is not able to provide the data to quickly respond to congressional inquiries, it may lose stakeholder support.	Low	Low	1	None required. Risk is minimal.	System is primarily in the steady-state phase of its life cycle. Risk is continuous and will be regularly monitored.	10 Jan 2013: Risk initially identified.
User access	10 Jan 2013	17) Security	If user access is not well maintained, unauthorized users may have access to sensitive data. ITDS contains patient data and prognostic data. The need for confidentiality of the information in ITDS makes the risk level high.	H=2	Low	2	Laura Lee Hope 301-443-1234	Classification of users is being reviewed currently and will be finalized by March 1, 2014.	10 Jan 2013: Risk initially identified.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment
As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Super users	10 Jan 2013	17) Security	If too many users have access to the system as super users, sensitive data may become accidentally corrupted. The need for the availability of accurate, comprehensive information makes the risk level medium.	Medium	Medium	4	Laura Lee Hope 301-443-1234	Classification of users is being reviewed currently and will be finalized by March 1, 2014.	10 Jan 2013: Risk initially identified. 17 Jan 2013: No risk occurrence. Continue monitoring. 24 Jan 2013: No risk occurrence. Continue monitoring. 31 Jan 2013: No risk occurrence. Continue monitoring. 7 Feb 2013: No risk occurrence. Continue monitoring. 14 Feb: No risk occurrence. Continue monitoring
System integrity	10 Jan 2013	17) Security	If the Information Security considerations have not been adequately addressed, then confidentiality, availability and integrity of the systems could be impacted.	Medium	High	6	Capt. Mark Twain will discuss C&A with the ISSO.	The investment is closely monitored for NIST 800-53 compliance. HHS is implementing specific security training in FY2013 for those employees and contractors with significant security responsibilities.	10 Jan 2013: Risk initially identified. 17 Jan 2013: Training on schedule. Continue monitoring. 24 Jan 2013: Training on schedule. Continue monitoring. 31 Jan 2013: Training on schedule. Continue monitoring. 7 Feb 2013: Training on schedule. Continue monitoring. 14 Feb: Training on schedule. Continue monitoring

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment
As of February 14, 2013

Risk Name	Date Identified	Risk Category	Description	Probability of Occurrence	Impact	Risk Magnitude	Risk Owner	Mitigation Plan	Date and Status
Privacy	10 Jan 2013	18) Privacy	If the privacy issues have not been addressed, then patient information, employee information, and other sensitive information may be compromised.	Medium	High	6	Capt. Mark Twain will discuss PIA with the IHS Privacy Officer.	Make employees and contractors aware of proper use of systems and privacy protection. Implement and maintain adequate controls to protect privacy as mandated in NIST 800-66 and 800-53. An IHS HIPPA privacy officer conducts awareness program. HIPPA officer conducts awareness program. Investment conducts annual privacy impact assessment.	10 Jan 2013: Risk initially identified. 17 Jan 2013: Training on schedule. Continue monitoring. 24 Jan 2013: Training on schedule. Continue monitoring. 31 Jan 2013: Training on schedule. Continue monitoring. 7 Feb 2013: Training on schedule. Continue monitoring. 14 Feb: Training on schedule. Continue monitoring.
Staff expertise	10 Jan 2013	19) Project Resources	If staff members do not have the right expertise, maintenance activities may be delayed and costs may increase.	Low	Medium	2	None required	Staff has demonstrated appropriate capability, although depth in experience is lacking.	10 Jan 2013: Risk initially identified.
Staff turnover	10 Jan 2013	19) Project Resources	If there is major staff turnover (either government or contractor staff), maintenance activities may be delayed as replacement personnel are oriented and educated.	Low	Medium	2	None required	Staff has undergone major turnover in the past year, and training and project orientation have proven adequate for transition. New staff qualifications are carefully reviewed for appropriate expertise.	10 Jan 2013: Risk initially identified. 25 Jan 2012: Risk has been mitigated.