



Indian Health Service

The Federal Health Program for American Indians and Alaska Natives

MANAGING CAPITAL INVESTMENTS AT THE INDIAN HEALTH SERVICE

A "HOW-TO" GUIDE TO RISK MANAGEMENT

JULY 2007

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.

Contents

- PURPOSE 1
- THE BASICS 2
 - What Is Risk? 2
 - What Is Risk Management?..... 2
 - How Do You Manage Risk?..... 2
- DRAFT A RISK MANAGEMENT PLAN 3
- ASSESS YOUR RISK..... 4
- TRACK AND REPORT PROGRESS..... 5
 - Executing Risk Management Activities..... 5
 - Reporting Risk Management Progress..... 6
 - Reevaluating Project Risk 6
- RISK MANAGEMENT ROLES AND RESPONSIBILITIES 7

- APPENDIX A. RISK MANAGEMENT PLAN TEMPLATEA-1
- APPENDIX B. CONDUCTING AN OPEN AND COMPREHENSIVE RISK REVIEWB-1
- APPENDIX C. SAMPLE RISK INVENTORY AND ASSESSMENT C-1
- APPENDIX D. TRACKING AND REPORTING RISK AND RISK MANAGEMENT D-1

Figures

- Figure 1. Steps of Risk Management..... 1
- Figure 2. The Risk Management Process..... 3

A “How-To” Guide to Risk Management

PURPOSE

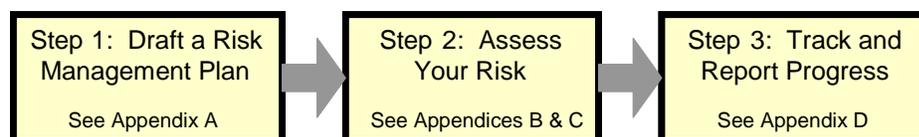
This guide is intended to be used by project managers and project team members to manage the risks associated with their projects.¹ The purpose of this guide is to provide a basic, easy, step-wise method for managing the risks associated with a project; a method that is consistent with federal and Indian Health Service (IHS) requirements. *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, ANSI/PMI 99-001-2004 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. To ensure the lowest possible risk in the performance of project efforts, the established goals for risk management should be to:

- 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 going into a step-by-step approach to managing risks, following the steps shown in Figure 1.

Figure 1. Overview of Risk Management



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.”

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. Appendix D shows how to report and track progress in mitigating the risks.

THE BASICS

What Is Risk?

A risk is an uncertain event or condition that, if it occurs, has a positive or negative affect on a project objective, such as time, cost, scope, or quality (i.e., where the project time objective is to deliver in accordance with the agreed-upon schedule; where the project cost objective is to deliver within the agreed-upon cost, etc. 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.

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

How Do You Manage Risk?

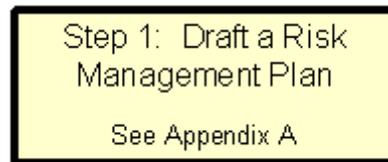
The appropriate level of risk management for any project depends on many factors (e.g., size, complexity, life-cycle phase, and stability) and determining that level requires candid management judgment. For example, a stable, straightforward application using established technology in the maintenance 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.

² *A Guide to the Project Management Body of Knowledge*, Third Edition (PMBOK Guide), ANSI/PMI 99-001-2004, Project Management Institute, Inc, Newton Square, PA, 2004.

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. One question in the latest Exhibit 300 asks if there is a risk management plan for each project, whether in the development, modernization or enhancement phase, or in steady state operations phase. Another question asks for the date of each project's risk management plan.

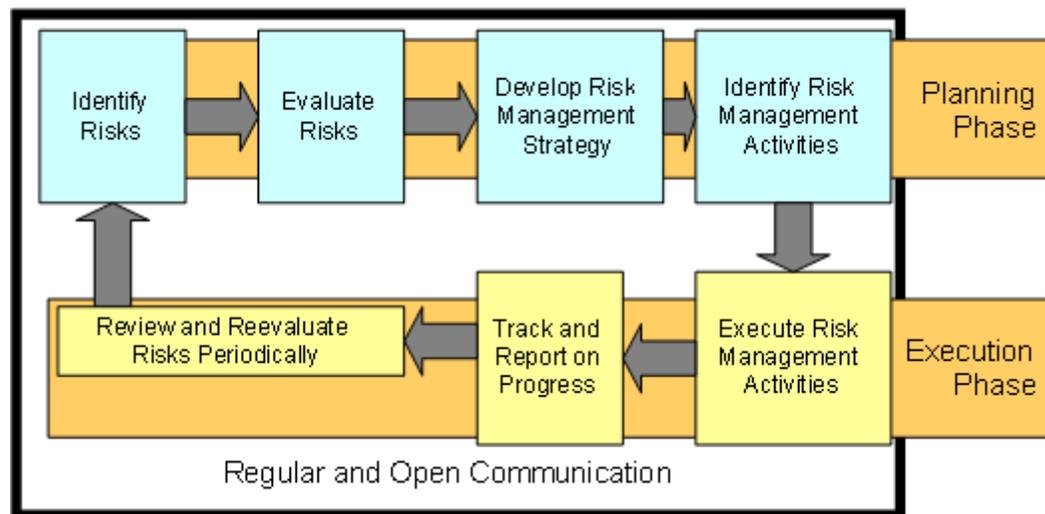
No one risk management approach is appropriate for all projects. Managers of smaller projects can profitably use elements of these risk management guidelines without the administrative burden of reporting risks to OMB. Those subject to OMB or HHS oversight *must* satisfy OMB requirements; risk status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

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 second four 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*.

Figure 2. The Risk Management Process



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 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 parties.

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

ASSESS YOUR RISK

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:

Step 2: Assess
Your Risk
See Appendices B & C

- *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.
- *Evaluate risks.* 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.
- *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 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 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.

- *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 review 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. A guide for reporting on risk management and risk management progress that follows the guidance that OMB required for reporting in the Exhibit 300 is presented in Appendix D. It includes a checklist to ensure complete compliance with OMB reporting requirements.

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, their risk management strategies, and the status of the risk management strategies. Providing similar information for projects that are not subject to HHS review, and therefore not in the PMT, is desirable as explained in Appendix D.

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

An independent and 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.

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	<u>Date</u>	Initial Draft	

TABLE OF CONTENTS

I. Purpose	1
II. Background	1
A. Organizational Mission	2
B. Project Description	2
III. The Project Name Risk Management Process	2
A. Planning Phase	3
B. Execution Phase	10
IV. Risk Management Roles and Responsibilities	12
A. Project Manager	13
B. Risk Owner	13

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 raise their health status to the highest possible level. The IHS currently provides health services to approximately 1.5 million American Indians and Alaska Natives who belong to more than 557 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.

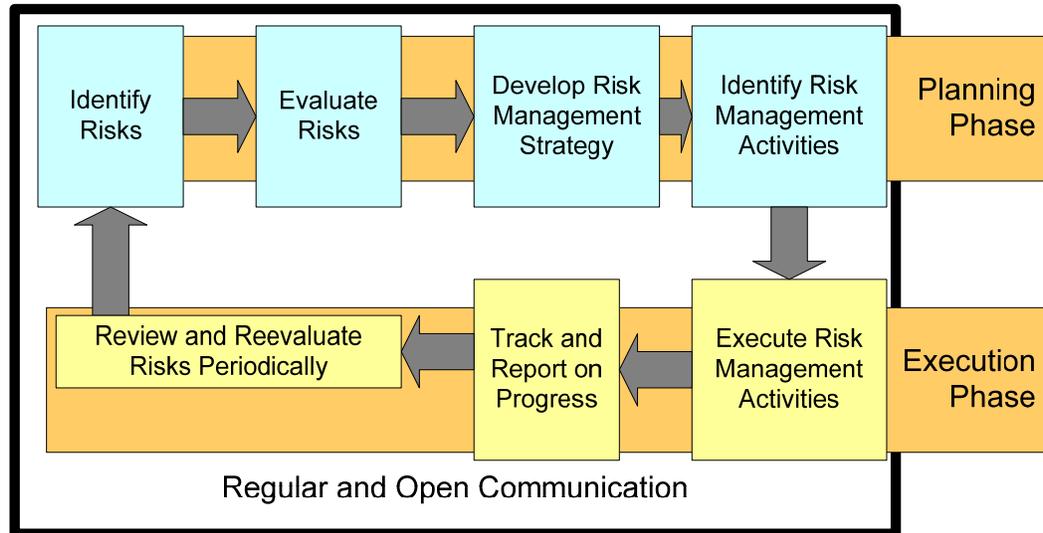
III. THE PROJECT NAME RISK MANAGEMENT PROCESS

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



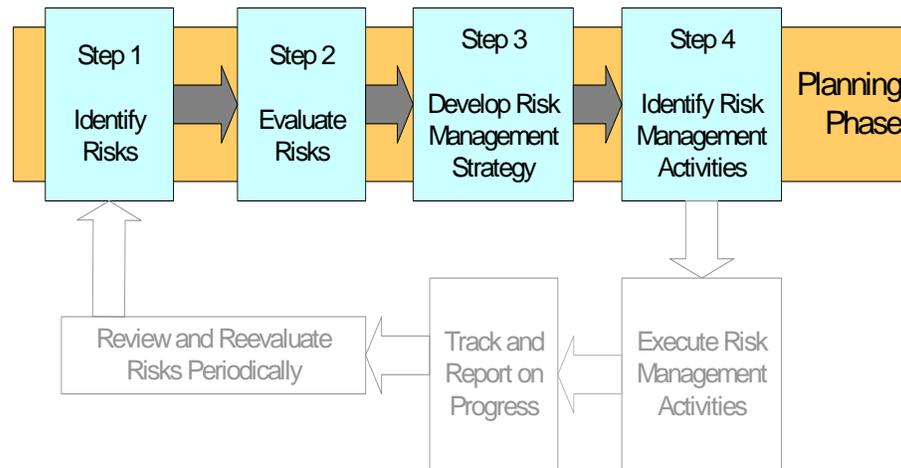
A. Planning Phase

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



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, successful transition to the new system will be jeopardized.”

“If the acquisition process does not include detailed selection criteria and an evaluation plan, 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; Risk Impact times Risk Probability of Occurrence = Risk Magnitude; which is used by the portfolio management tool (PMT) that HHS and IHS use to evaluate the projects 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 risk's potential impact and the estimated probability of the risk occurring. 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 estimating the degree of impact on the project if the risk is not mitigated. Table 2 provides the ratings and guidelines for the estimated probability that the risk situation will occur.

Table 1. Degree of Impact

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

Table 2. Probability of Occurrence

Probability	Rating	Guideline
High	3	Likely to occur
Medium	2	May occur
Low ^a	1	Unlikely to occur

^a A low probability of occurrence is entered as “basic” in the HHS PMT.

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

$$\text{Risk Magnitude} = \text{Impact} \times \text{Probability.}$$

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

Table 3. Risk Magnitude

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

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., 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 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 through 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.

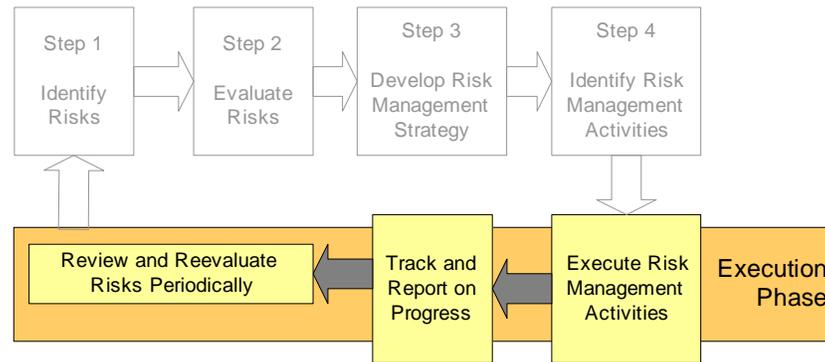
The risk owner tracks and reports on progress toward risk management at predetermined risk review sessions conducted by the project team—at least monthly.

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



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 independent and comprehensive review of the risk posture of the [Project Name](#). 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

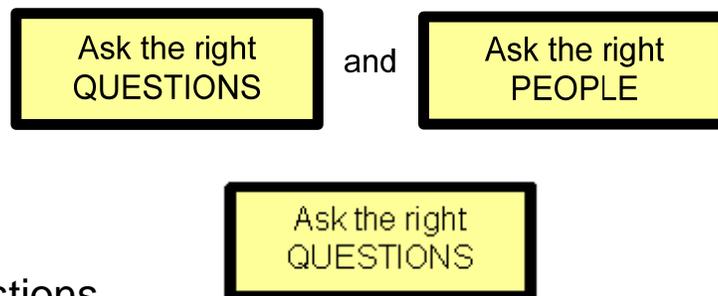
APPENDIX B. CONDUCTING AN OPEN AND COMPREHENSIVE RISK REVIEW

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

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, requires a 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, comprehen-

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.

sive set of risk categories that are useful to project managers as a starting point for defining their project risks.⁶

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.

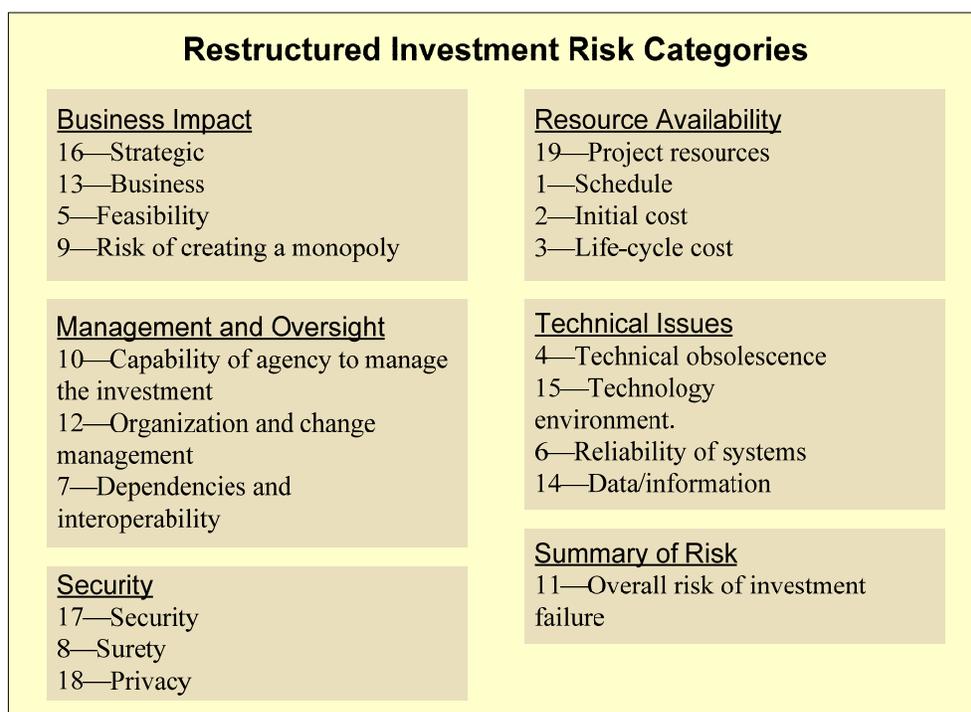
Figure B-2. OMB's 19 Risk Categories

Risk Categories for All Investments	Risk Categories for IT Investments
1) Schedule	12) Organizational and change management
2) Initial cost	13) Business
3) Lifecycle cost	14) Data/information
4) Technical obsolescence	15) Technology
5) Feasibility	16) Strategic
6) Reliability of systems	17) Security
7) Dependency and interoperability	18) Privacy
8) Surety (asset protections)	19) Project resources
9) Risk of creating a monopoly	
10) Capacity 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 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.

⁶ During the years prior to the preparation of the OMB Exhibit 300 for the FY08 budget, OMB provided comprehensive risk reporting instructions. HHS still requires that reporting as part of its project prioritization process for projects that it reviews. A guide to tracking and reporting risk management activities to meet these requirements is included in Appendix D.

Figure B-3. Restructured OMB Risk Categories



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
Business Impact	16—Strategic	<p>Risk associated with strategic/government-wide goals (e.g., President's Management Agenda and e-Gov initiative 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.</p> <p>Risk that the proposed alternative fails to result in the achievement of those goals or in making contributions to them.</p> <p>Risk that strategic goals and objectives, including PMA goals or HHS priorities, may change.</p> <p>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.</p> <p>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).</p>
	13—Business	<p>Risk associated with the validity of the business case for the project, the completeness and validity of the specified functional requirements, and the need for reengineering subject business processes.</p> <p>Risk that the business goals of the program or initiative will not be achieved.</p> <p>Risk that the program effectiveness targeted by the project will not be achieved.</p>
	5—Feasibility	<p>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.</p> <p>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.</p>
	9—Risk of creating a monopoly	<p>Risk associated with the over-reliance on a particular vendor or on proprietary or specialty software that would limit project expansion or flexibility.</p>
Resource Availability	19—Project resources	<p>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.</p> <p>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).</p> <p>Risk that appropriate training will not be available in a timely fashion.</p>
	1—Schedule	<p>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.</p> <p>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.</p>

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations
	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.
	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.
Management and Oversight	10—Capability of agency to manage the investment	<p>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.</p> <p>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.</p> <p>Also relates to the degree to which program plans and strategies exist and are realistic and consistent.</p>
	12—Organization and change management	<p>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.</p> <p>Risk associated with bypassing, lack of use, improper use, or adherence to new systems and processes due to organizational structure and culture; inadequate training.</p>
	7—Dependencies and interoperability	<p>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).</p> <p>Risk associated with the requirement for the project to operate in concert with other programs. Include related schedule and funding concerns.</p> <p>Risk is increased if the success of a project is directly linked to the success/ implementation or on-going maintenance of other systems.</p>

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations
Technical Issues	4—Technical obsolescence	<p>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.</p> <p>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.</p>
	15—Technology	<p>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.</p> <p>Risk associated with immaturity of commercially available technology.</p> <p>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.</p>
	6—Reliability of systems	<p>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.</p> <p>Risk of inability of the system to provide planned and desired functionality.</p>
	14—Data/information	<p>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.</p> <p>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).</p>
Security	17—Security	<p>Risk associated with the security/vulnerability of systems, websites, information and networks; risk of intrusions and connectivity to other (vulnerable) systems</p> <p>Risk associated with the misuse (criminal/fraudulent) of information</p> <p>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.</p> <p>[Note: This risk category must include in the risk description the level of risk (high, medium, basic/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.]</p>

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations
	8—Surety	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.
	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.
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.

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.

A unique identifier for each risk is in the first column, consisting of a four digit number that has the fiscal year that the risk was identified as the first two digits and a sequential two digit number as the last two digits of the risk identifier.

Within an area of risk, there can be more than one risk.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment April 1, 2007							
Risk ID/ Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Mag- nitude	Risk Owner	Notes
0704 Mar 19, 2007	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.
0705 Mar 19, 2007	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.
0706 Mar 19, 2007	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.
0709 Mar 19, 2007	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.
0504 9/29/2005	4) Technical obsolescence	Oracle migration. 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.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

April 1, 2007

Risk ID/ Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Mag- nitude	Risk Owner	Notes
0711 Mar 19, 2007	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.
0711 Mar 19, 2007	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.
0505 9/29/2005	6) Reliability of systems	Software/hardware reliability. 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.
0506 9/29/2005	6) Reliability of systems	Shared system. If a change is made in the hardware or software to accommodate other work without evaluating its impact on all systems, ITDS may fail.	Low	Medium	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.
0708 Mar 19, 2007	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.
0714 Mar 19, 2007	8) Surety Considerations	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.	
0703 Mar 19, 2007	9) Future Procurements	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.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

April 1, 2007

Risk ID/ Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Mag- nitude	Risk Owner	Notes
0707 Mar 19, 2007	10) Project Management	Project management skills. 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 2007.
0201 Feb 15, 2002	11) Overall project failure	If Inadequate attention is paid to monitoring cost, schedule, and performance goals, then the investment may be impacted.	High	Low	3	Capt. Mark Twain will monitor EVM variances monthly.	COTS product; planned use similar to previous use
0504 9/29/2005	12) Org/Change Management	No organization and change management risks have been identified. ITDS is used daily by multiple users in many offices.	Low	Low	1	None required	ITDS is well established among users and is primarily in the steady-state phase of its life cycle.
Feb 15, 2002	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.
0602 Mar 27, 2006	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.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

April 1, 2007

Risk ID/ Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Mag- nitude	Risk Owner	Notes
0501 9/29/2005	13) Business	Poorly defined field names. 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, 2007. 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, 2007.
0712 Mar 19, 2007	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.
0507 9/29/2005	14) Data/Info	Data requirements. If data requirements are unclear to data suppliers, data collected may be inconsistent, incomplete, and inaccurate. (See risk 0502, 13—Business.)	Medium	Medium	4	Flossie Bobbsie 505-248-1234	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. The efforts underway for risks 0502, 0503, and 0504 should mitigate this risk.
0710 Mar 19, 2007	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.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

April 1, 2007

Risk ID/ Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Mag- nitude	Risk Owner	Notes
0701 Mar 19, 2007	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.
0601 Mar 27, 2006	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.
0509 9/29/2005	17) Security	User access. 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.	Low	H=2	2	Laura Lee Hope 301-443-1234	Classification of users is being reviewed currently and will be finalized by March 1, 2008.
0508 9/29/2005	17) Security	Super users. 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, 2008.
0713 Mar 19, 2007	17) Security	If the Information Security considerations have not been adequately addressed, then confidentiality, availability and integrity of the systems could be impacted.	High	Medium	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 FY2007 for those employees and contractors with significant security responsibilities.

Infrared Terosis Detection System (ITDS) Risk Inventory and Assessment

April 1, 2007

Risk ID/ Date Identified	Area of Risk	Description	Impact	Probability of Occurrence	Risk Mag- nitude	Risk Owner	Notes
0715 Mar 19, 2007	18) Privacy	If the privacy issues have not been addressed, then patient information, employee information, and other sensitive information may be compromised.	High	Medium	6	Capt. Mark Twain will discuss PIA with the IHS Privacy Officer.	<p>Make employees and contractors aware of proper use of systems and privacy protection.</p> <p>Implement and maintain adequate controls to protect privacy as mandated in NIST 800-66 and 800-53.</p> <p>An IHS HIPPA privacy officer conducts awareness program.</p> <p>HIPPA officer conducts awareness program. Investment conducts annual privacy impact assessment.</p>
0503 9/29/2005	19) Project Resources	Staff expertise. If staff members do not have the right expertise, maintenance activities may be delayed and costs may increase.	Medium	Low	2	None required	Staff has demonstrated appropriate capability, although depth in experience is lacking.
0502 9/29/2005	19) Project Resources	Staff turnover. If there is major staff turnover (either government or contractor staff), maintenance activities may be delayed as replacement personnel are oriented and educated.	Medium	Low	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. Risk has been mitigated as of September 29, 2005.

APPENDIX D. TRACKING AND REPORTING RISK AND RISK MANAGEMENT

Risk management includes assessment of risk, development and execution of risk management strategies, and monitoring of progress, that is, tracking and reporting on project risk and progress toward mitigating it. This appendix addresses the tracking and reporting of risk management activities.

Two kinds of tracking and reporting are important for effective project risk management:

- Tracking and reporting for internal project management, communication, and management of stakeholder expectations.
- Tracking and reporting of risk management activities for external reporting to OMB or other oversight authorities.

Internal Reporting Requirements

Appropriate reporting frequency and internal project team tracking and reporting procedures can be different for each project. Internal reporting procedures for your project should be developed and described in the project's risk management plan. The elements of a risk management plan are described in Appendix A. It will probably be easiest if the internal reporting formats follow the external reporting formats presented in this appendix but they may be more comprehensive.

External Reporting Requirements

According to OMB's BY2008 guidance, the Exhibit 300 for a project for which OMB has oversight authority must indicate that the project has a risk management plan and must provide the date of the plan. OMB reserves the right to review the risk management plan. To prepare for such a review, the reporting guidance that OMB has used in the past serves as a good indication of what it is looking for when it reviews the risk management artifacts. The instructions for risk reporting that were part of the guidance for preparing the BY2007 OMB Exhibit 300 are reproduced in Figure D-1.

Figure D-1. OMB Exhibit 300 Instructions for Risk Management

I. F. RISK INVENTORY AND ASSESSMENT (ALL ASSETS)

In order to successfully address this issue on the business case and capital asset plan, you must have performed a risk assessment at the initial concept, included mandatory risk elements (*categories*) defined below and demonstrate active management of the risk throughout the life-cycle of the investment.

For all investments, both IT and non-IT, you must discuss each of the following risks and present your plans to eliminate, mitigate, or manage risk, with milestones and completion dates. If there is no risk to the investment achieving its goals from a risk category, indicate so. If there are other risks identified, please include them. Risk assessments should include risk information from all stakeholders and should be performed at the initial concept stage and then monitored and controlled throughout the life-cycle of the investment. Risk assessments for all investments must include: 1) schedule; 2) initial costs; 3) life-cycle costs; 4) technical obsolescence; 5) feasibility; 6) reliability of systems; 7) dependencies and interoperability between this investment and others; 8) surety (asset protection) considerations; 9) risk of creating a monopoly for future procurements; 10) capability of agency to manage the investment; and 11) overall risk of investment failure.

In addition, for IT investments, risk must be discussed in the following categories: 12) organizational and change management; 13) business; 14) data/info; 15) technology; 16) strategic; 17) security; 18) privacy; and 19) project resources. For security risks, identify under the Description column the level of risk as high, medium, or basic. What aspect of security determines the level of risk, i.e., the need for confidentiality of information, availability of information or the system, reliability of the information or system? Under the Current Status column, list the milestones remaining to mitigate the risk.

Date Identified	Area of Risk	Description	Probability of Occurrence	Strategy for Mitigation	Current Status
-----------------	--------------	-------------	---------------------------	-------------------------	----------------

1. What is the date of your risk management plan?

These instructions contain several important points:

- Every risk category must be considered, but every category need not have an identified risk. (In fact, it is unlikely that every project will have a risk in every category because of such differences as project life-cycle phase and complexity.) If no risk has been identified in a risk category, say so in the Description column and say why in a short sentence. Other columns should have “low” or “NA” or a short explanatory phrase to complete the entry. This way the reader will know the risk category has been considered.

- Risks identified in category 17, Security, require additional information in the Description column. Include the “level” (magnitude) of risk as high, medium, or basic (OMB uses the term “basic” for risks of low magnitude), and say why the risk is classified that way, following the examples in paragraph 3 of the instructions.
- The status should always indicate a date, either the date that the risk was mitigated (which would be the date of the assessment if the risk category is NA) or the dates of risk management activities and when the risk will be mitigated.
- Proper formats for statements of risks and for risk management strategies are included in the Risk Management Plan Template, Appendix A.
- If entering data into the HHS PMT, do not leave a Probability of Occurrence cell or an Impact cell empty. If the risk is NA, indicate that the probability of occurrence is low or basic and that the impact is low or basic.

Check Sheet for Effective OMB Risk Management Compliance

Use the check sheet in Table D-1 to evaluate and improve your reporting responses.

Table D-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say if reporting to OMB in the Exhibit 300
Risk Management Plan Date			
No date for a risk management plan is given.		Prepare a risk management plan.	Say that a risk management plan is being developed, and specify the date it will be completed.
A risk plan date is given but it is apparent that the plan is inadequate.		Revise or update the risk management plan.	Cite the date of the current plan, but say it is being updated and specify the date it will be completed.
Risk Inventory Matrix—Date column			
All risks are identified on the same date.		Revise the risk management plan to encourage ongoing risk identification.	Cite the date of the current plan, but say it is being updated to include ongoing risk identification and specify the date it will be completed.
All risks have been identified before the date of the risk management plan. (No risks have been identified under the plan.)		Conduct a comprehensive risk identification session. Revise the risk management plan to require periodic risk evaluation and ongoing risk evaluation.	Cite the date of the current plan, but say it is being updated to include more regular risk identification and specify the date it will be completed.

Table D-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say if reporting to OMB in the Exhibit 300
All risks are identified on the same date as the risk management plan.		Conduct a comprehensive risk identification session if a year has passed since the date. Revise the risk management plan to require periodic risk evaluation and ongoing risk evaluation.	Cite the date of the current plan, but say it is being updated to include more regular risk identification and specify the date it will be completed.
Risk Inventory Matrix—Area of Risk column			
All 19 OMB risk categories are not included.		Conduct a comprehensive risk identification session to ensure that all 19 risk categories are considered. Revise the risk management plan to require periodic, comprehensive risk evaluation.	Each OMB risk category must be shown to have been considered. If no risks were identified in a category, say so. If a risk or risks were identified, show them in the OMB 300 risk matrix. Cite the date of the current plan, but say it is being updated to include more comprehensive risk identification and specify the date it will be completed.
One and only one risk is identified for each risk category, implying that risk identification has been done to satisfy the requirements of the OMB 300 rather than for effective project control. It is unusual that a project has legitimate risks in every category.		Conduct a comprehensive risk identification session to ensure that all 19 risk categories are considered. Revise the risk management plan to require periodic, comprehensive risk evaluation.	Each OMB risk category must be shown to have been considered. If no risks were identified in a category, say so. If more than one risk was identified in a particular category, show them.
There is never more than one risk listed for any category.		If more than one risk is identified for any risk category, show them all.	Include all risks identified for each risk category.
Risk Inventory Matrix—Description column			
The Description column is blank, or it contains NA, none, or other indication of no risk having been identified in a particular risk category.		Update the risk management plan to manage risk categories without risks.	Say that no risks have been identified in a particular risk category and briefly say why. For example: "No initial cost risks have been identified because the system is stable and is in the O&M phase of its life cycle." The remaining columns may be blank or contain "NA" or "none." An exception is the Strategy for Mitigation column, which may contain a short statement of what is being done to make sure no risks develop in this risk category.

Table D-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say if reporting to OMB in the Exhibit 300
The Description column contains only a word or two or a sentence fragment that is too short to effectively communicate what the risk is and why.		Restructure the risk statements into cause-and-effect statements within the project's risk management process. Update the risk management plan to improve risk definition.	State each risk as a cause-and-effect statement describing what the risk is and why. For example: "If the data in the legacy system are inaccurate or incomplete, they cannot become an effective basis for the new system. "
The Description column contains a lengthy explanation of the risk or contains material such as mitigation strategies that belong in other columns.		Shorten the risk statements into cause-and-effect statements within the project's risk management process. Update the risk management plan to improve risk definition.	State each risk as a cause-and-effect statement describing what the risk is and why. For example: "If the data in the legacy system are inaccurate or incomplete, they cannot become an effective basis for the new system. "
The Description column for 17—Security risk does not rate the risk level as high, medium, or basic, nor does it say what aspect of security determines the level of risk. (See OMB's instructions for "Risk Inventory and Assessment" for details.)		Rate each 17—Security risk level as high, medium, or basic. ("Risk level" is undefined by OMB.) Determine the aspect of security that determines the risk, for example, the need for confidentiality of the information, availability of the information or the system, or reliability of the information or system. (Risk level is not necessarily the same as the risk's probability of occurrence, required in the next column in the matrix.)	Include the risk level rating and reason in the Description Column for 17—Security only.
Risk Inventory Matrix—Probability of Occurrence column			
All probability of occurrence ratings are the same or almost so.		Reconsider the risk ratings to provide a useful distribution of high-, medium-, and low-rated risks. Update the risk management plan to allow different actions to be taken for different probabilities of risk occurrence.	Cite properly distributed risk ratings.
Agency management or the OMB 300 entry tool requires a multi-step risk rating system (perhaps combining probability of occurrence with risk impact), but OMB requires only probability of occurrence.		Adjust the risk management plan to accommodate a multi-step risk rating process if required by agency management or the tool used to manage OMB 300 information.	Enter multi-step risk ratings for each risk as required.
Risk Inventory Matrix—Strategy for Mitigation column			
Statements about the mitigation strategy are too short to explain what the strategy is.		Rewrite the mitigation strategy statements to be more effective in explaining the approach to be used to mitigate the risk.	Provide an effectively worded statement that explains the strategy in a few sentences (usually fewer than 50 words).

Table D-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say if reporting to OMB in the Exhibit 300
Statements about the mitigation strategy are lengthy and detailed.		Rewrite the mitigation strategy statements to be more concise.	Provide an effectively worded statement that explains the strategy in a few sentences (usually fewer than 50 words).
Risk Inventory Matrix—Current Status as of the Date of this Exhibit column			
The Current Status entry is too brief or too complex to be useful in describing the actual current status of mitigation activities. Dates for specific mitigation milestones are omitted.		Develop action steps to execute the mitigation strategy and assign responsibility. Monitor results regularly. Expand the risk management plan to include mitigation execution and tracking processes if they are lacking. (The object of this column is to reassure the reader that the mitigation strategy is being executed and results tracked.)	List two to four (maybe more) steps to be taken toward mitigating the risk. Include a milestone date for each step. If necessary, use less specific time measures (second quarter, beginning of FY08, etc.). Be as specific as possible. Cite the date of the current plan, but say it is being updated to strengthen risk mitigation execution and tracking. Cite the date the revised plan will be completed.