MANAGING CAPITAL INVESTMENTS
AT THE NATIONAL INSTITUTES OF HEALTH

A "HOW-TO" GUIDE TO RISK MANAGEMENT

JULY 2006

OFFICE OF THE DEPUTY CHIEF INFORMATION OFFICER
10401 FERNWOOD ROAD
BETHESDA, MD 20817
301-402-4465

Contents

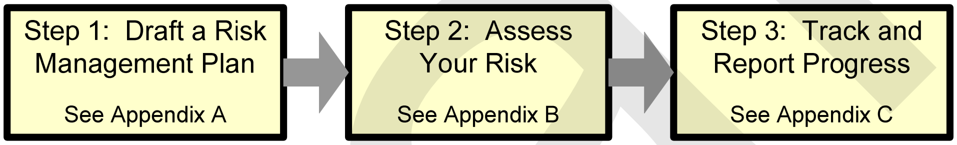
Figures

A “How-To” Guide to Risk Management

This guide is intended to be used by project managers and project team members to manage and mitigate the risks associated with their projects.[1] The purpose of this guide is to provide an easy, step-wise method for managing the risks associated with a project—a method that is consistent with federal and NIH requirements.

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

Figure 1. Steps of Risk Management


Step 1: Draft a Risk Management Plan
See Appendix A
Step 2: Assess Your Risk
See Appendix B
Step 3: Track and Report Progress
See Appendix C

Appendix A contains a template for a draft risk management plan. Appendix B tells how to conduct a comprehensive risk review, and Appendix C 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 effect on a project objective.[2]

What Is Risk Management?

Risk management is an organized method of identifying and measuring the risk associated with a project 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

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

[2] Office of the Chief Information Officer, Office of the Assistant Secretary for Budget, Technology and Finance, Department of Health and Human Services, *CPIC Procedures Appendices*, December 30, 2005, Document No. HHS-OCIO-2005-005P-A.

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—size, complexity, life-cycle phase, and stability are some examples—and determining that level requires considerable 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 so that, in the event of an inquiry, OMB can 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 C.

Draft a Risk Management Plan

Step 1: Draft a Risk Management Plan

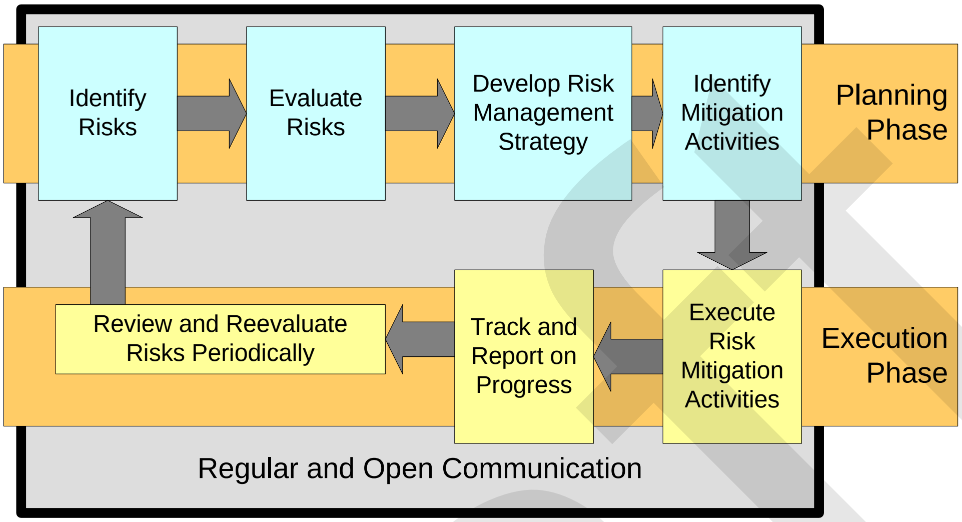
See Appendix A

The risk management plan presents the documented process and activities that will take place to execute the risk management process model.

The risk management planning process begins with the selection of a risk management process model. For projects being executed in the National Institutes of Health (NIH), the NIH Office of the Deputy Chief Information Officer (CIO) recommends the model 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 NIH. The first four activities of the risk management process model depicted in the figure, designating the planning phase and presented in the top row, provide the actions required to complete step 2 of Figure 1, *assess your risk*. The second four activities of the risk management process model, designating the execution phase and presented in the bottom row of the figure, provide the actions required to complete step 3 of Figure 1, *track and report progress*.

[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 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.

Figure 2. The Risk Management Process


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

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 mitigate the risks, and how mitigation actions will be developed, monitored, and reported. A template for a risk management plan is presented in Appendix A. The level of funding for 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

Step 2: Assess Your Risk

See Appendix B

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: both as an ongoing part of project management, and comprehensively as a periodic process to assure that new risks are fully recognized.
- *Evaluate risks.* Each risk should be rated on the likelihood that the risk will occur and its potential impact on the project if it does occur. Normally this rating is high, medium, or low for both probability of occurrence and for the potential impact. A level of magnitude for the overall risk can be

computed by assigning a numerical score to each risk level and multiplying the numerical score of the risk likelihood of occurrence by its potential impact score. By formally evaluating the risks, 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 or mitigating each risk should be determined. The mitigation strategy is expressed in a short statement that describes the approach to mitigating the risk. For a risk with a high magnitude, a specific risk owner may be assigned to manage the risk and its mitigation activities.
- *Identify mitigation activities.* The project manager, or risk owner if one is assigned, should develop an approach and action plan to implement the mitigation strategy.

A guide for conducting an open and comprehensive risk review is presented in Appendix B.

TRACK AND REPORT PROGRESS

Step 3: Track and Report Progress

See Appendix C

The execution phase of the risk management process model provides a periodic review of the status of risk mitigation 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 mitigation progress that follows the guidance that OMB required for reporting in the Exhibit 300 is presented in Appendix C. It includes a checklist to ensure complete compliance with OMB reporting requirements.

Executing Risk Mitigation Activities

Overall execution of the risk mitigation strategy and the corresponding mitigation plans is managed by the risk owner. Mitigating the risks is tracked against the risk mitigation plan developed for each risk. HHS uses a commercial software package, ProSight, as its portfolio management system to track its information technology investments. ProSight provides forms to use for reporting project risks, their levels of magnitude, their mitigation strategies, and the status of the mitigation strategies.

Reporting Risk Mitigation Progress

Risk owners regularly report on their progress in implementing the risk mitigation strategies and the current status of the risk mitigation 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.

Most projects 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 of plus or minus 10 percent or more.

Reevaluating Project Risk

An independent and comprehensive review and assessment should occur at least once per year. This annual review can be timed to provide current comprehensive information to assist the project manager with preparing the OMB Exhibit 300.

RISK MANAGEMENT ROLES AND RESPONSIBILITIES

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

The risk owner is responsible for overall execution of the risk mitigation strategy and the corresponding risk mitigation plans, 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 mitigation 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.[1] 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."

[1] 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.

Risk Management Plan for Project Name, Month Year

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 system. Specifically, this plan provides procedures that

- serve as a basis for identifying, documenting, analyzing, and prioritizing risks associated with the project and for developing mitigation strategies to handle those risks and
- enable National Institutes of Health (NIH), Institute/Center (I/C), and Organization Unit executives and the project team to monitor the health of the system throughout its life cycle.

II. BACKGROUND

Describe the mission of the I/C. The mission of the I/C can probably be extracted from the I/C 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.

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.

A. About Project Name

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

B. Importance of Managing Risks

Describe why managing risk is important to this project. Cite federal authorities and guidance for risk management. See the example below.

Federal central management authorities agree that management of risk is crucial to effective system and capital asset management. The Office of Management and Budget (OMB) addresses the risk associated with large capital programs directly. Specifically, OMB Circular A-11, Exhibit 300, requires that a major IT project have a documented risk management plan and a risk management process. More important, risks must be identified and managed if a project is to be a success.

Cite current NIH and I/C guidance for risk management or relevant principles for project management, if appropriate.

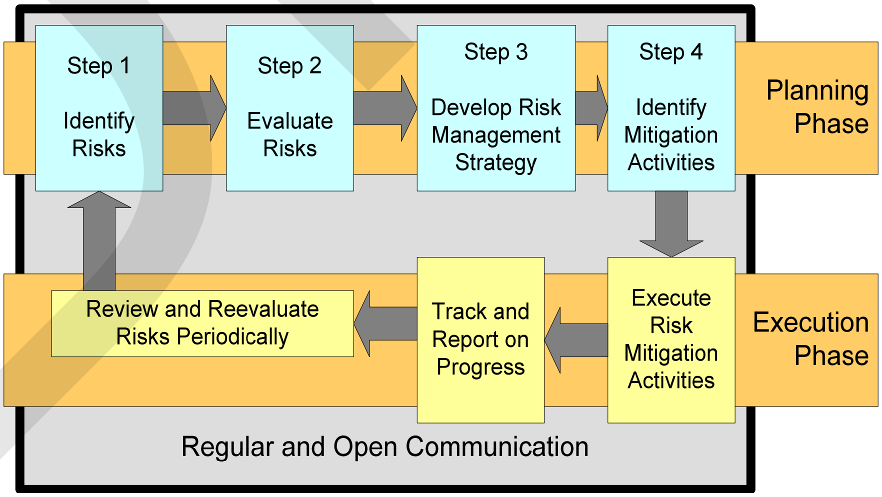
III. The Project Name Risk Management Process

Select a risk management model to be followed. Several are available, including one from the Software Engineering Institute of Carnegie Mellon University. We recommend the model developed by LMI because it identifies specific steps to be followed and it is easily adaptable to federal government compliance requirements.[2] This template is based on the LMI model.

Describe the model and show it graphically. The following is an example of a risk management model description for the LMI model and model description.

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


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

[2] LMI is a not-for-profit consulting firm specializing in improving management within the federal government.

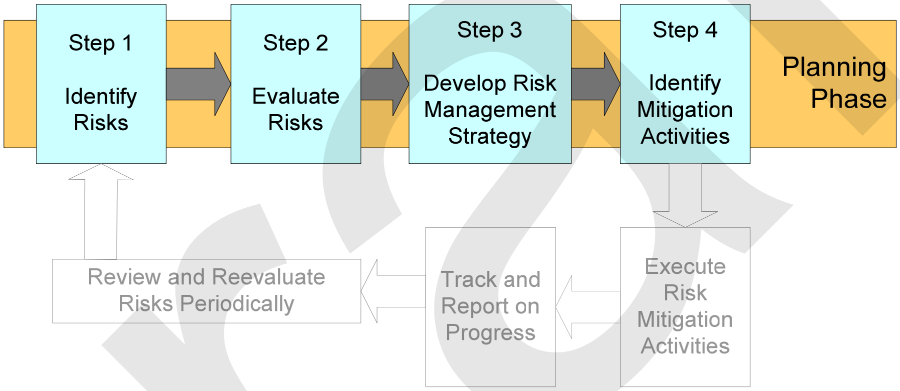
A. Planning Phase

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

- Identify risks
- Evaluate risks
- Develop risk management strategy
- Identify mitigation 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 Mitigation Activities
Planning Phase
Review and Reevaluate Risks Periodically
Track and Report on Progress
Execute Risk Mitigation Activities

1. Identify Risks

Define risk 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.

Risks should be stated in a “cause-and-effect“ format. 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.

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. 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 NIH, and it will not be legally defendable.“*

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: continuously by the project team and periodically through a comprehensive, independent risk assessment.

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 about the program.

Continuous risk identification processes 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 processes 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 process 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 system risks. For example, the review could correlate with the agency budget process and the update of the OMB Exhibit 300 submission. 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 ProSight, the portfolio management tool that HHS and NIH use to evaluate their major and tactical projects 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 mitigation of risks with a greater magnitude receives more management attention than the mitigation 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 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 ProSight portfolio management system.

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

Risk Magnitude = Impact × *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 system 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 I/C 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 a risk mitigation plan developed for it. Risks with a lower risk magnitude might be handled in a less intensive manner.*

- *Developing a risk mitigation 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 a mitigation plan.*

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 common risk management strategy is to mitigate the risk. Introduce mitigation strategies in a short paragraph. Give one or two examples that are relevant to your project. Say something like the following.

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

The mitigation strategy is a short statement that describes the approach to mitigating 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."*

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

> *"The program manager will implement the security protocols provided by NIH and NIST."*

Don't limit the definition of "mitigation." Any of these approaches could be a mitigation strategy:

- *Reducing the probability of risk occurrence and/or the impact on the project*
- *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.*

The mitigation strategy for each risk will be recorded and tracked in ProSight.

4. Identify Mitigation Activities

Describe how you plan to have mitigation plans developed by the risk owner (or whomever else might be assigned responsibility for developing the plans), and how mitigation 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 mitigation strategy. For example, for simple risk mitigation strategies, a list of actions with due dates and responsibilities may suffice. Or, for complex or high-magnitude risks, a detained plan for mitigation might be needed. Using Microsoft Project as a tool to help manage the risk mitigation project may be appropriate.

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

Once the mitigation strategy is approved by the project team, the risk owner will develop an approach and propose actions to execute the mitigation 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 mitigation actions will be assigned to specific individuals and formalized.

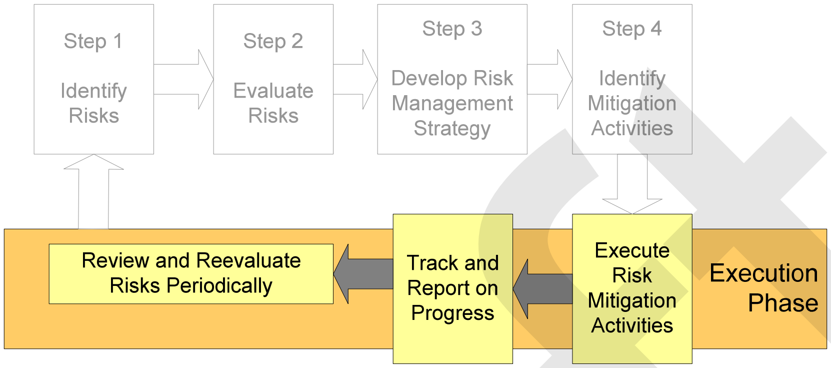
The risk owner tracks and reports on progress toward risk mitigation at predetermined risk review sessions conducted by the project team—at least monthly.

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 Mitigation Activities
Review and Reevaluate Risks Periodically
Track and Report on Progress
Execute Risk Mitigation Activities
Execution Phase

1. Execute Risk Mitigation Activities

Describe responsibilities for execution of the mitigation plans in a few paragraphs. Say something like the following.

Those responsible for executing the risk mitigation 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 mitigation strategy and the corresponding mitigation activities.

2. Track and Report on Progress

Describe how information on risks and mitigation plans will be tracked. Begin by stating something like the following.

Performance and progress on mitigating the risks are tracked against the risk mitigation plan. Progress against the mitigation 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 system, 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 mitigation strategies, mitigation activities, and progress toward mitigation should be available to appropriate staff and managers.

Don't forget to mention annual reporting to OMB and others.

Progress toward mitigating risks will be reported annually to senior Institute/ Center and NIH 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 Institute/Center 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 OMB Exhibit 300 update.

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, in addition to those described in *Capital Planning and Investment Control Policy and Guidelines*, issued by the Office of the CIO.

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 mitigation 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 mitigation 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.

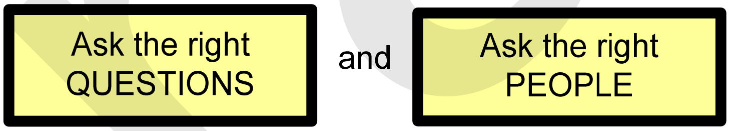
APPENDIX B. CONDUCTING AN OPEN AND COMPREHENSIVE RISK REVIEW

Risk management includes assessment of risk, development and execution of mitigation 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.[1] 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

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 mitigation 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-

[1] 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.[2]

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.

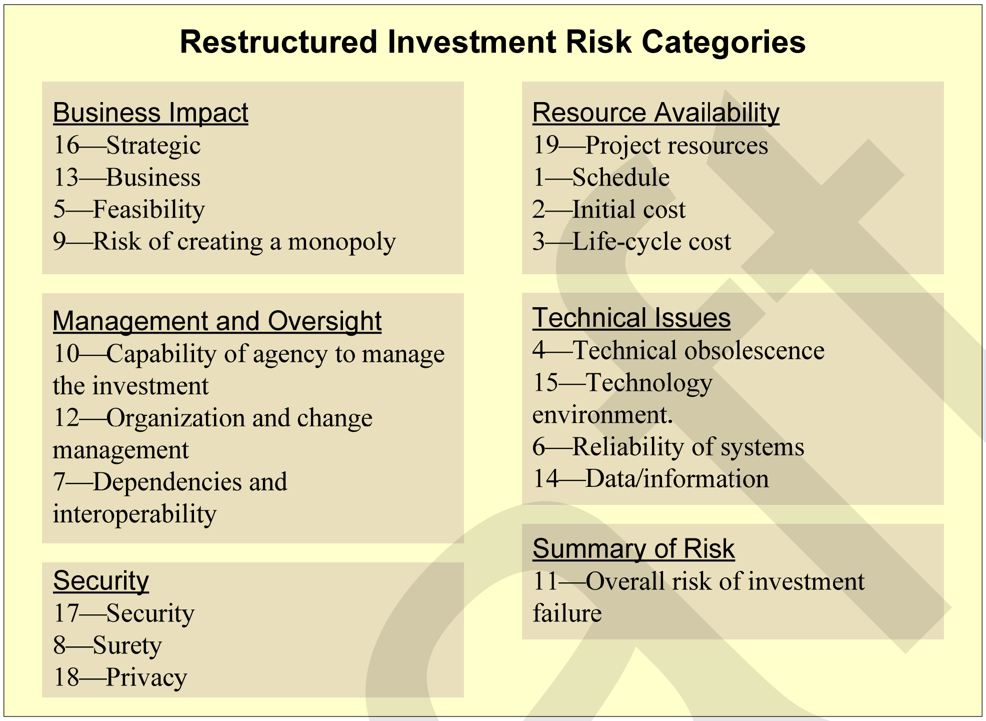
Figure B-2. OMB's 19 Risk Categories

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. We have found 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.

[2] 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. A guide to tracking and reporting risk management activities to meet these requirements is included in Appendix C.

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 environment.
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, we have found that it improves the ability of the risk assessment team to identify risks if the assessment starts with those areas that are broadest in scope. We recommend that the risk assessment leader start the assessment with Business Impact—the highest level, least technical of the risk areas—then address the other areas according to scope: Resource Availability, Management and Oversight, Technical Issues, and Security, the most narrow and specialized area. 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	Top management support and communication, consistency with strategic plans, high-level visibility with outside stakeholders such as OMB or Congress, and other political impacts.
	13—Business	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.
	5—Feasibility	Feasibility of the requirements from a technical and performance point of view and the organization's familiarity with the system life-cycle method used within the organization or as implemented by others.
	9—Risk of creating a monopoly	Overreliance on a particular vendor or on proprietary or specialty software that would limit project expansion or flexibility.

Table B-1. Order for Addressing Risks and Considerations

Risk area	Risk category	Considerations
Resource Availability	19—Project resources	Stability and adequacy of project staff and project budget for today and the future. Include resources that might be available from contractors.
	1—Schedule	Stability, reality, and validity. Include the cost or impact of not meeting the schedule.
	2—Initial cost	Adequacy 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	Adequacy 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.
Management and Oversight	10—Capability of agency to manage the investment	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.
	12—Organization and change management	Willingness and ability of the organization to accept the changes required by the project. Include the existence or adequacy of the change management plan, communications plan, and user training plan.
	7—Dependencies and interoperability	Dependence of the project on data from other systems and processes (existing and planned) and the requirement for the project to operate in concert with other programs. Include related schedule and funding concerns.
Technical Issues	4—Technical obsolescence	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.
	15—Technology	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.
	6—Reliability of systems	Defined response time and throughput requirements. Include system contingency plans, continuity of operations plans, disaster recovery plans and tests of those plans.
	14—Data/ information	Clarity, completeness, validity, sources, and feasibility of data requirements. Include data interface and data conversion complexities. Include data collection, storage, integrity, and availability.
Security	17—Security	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. Include information and system access concerns.
	8—Surety	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	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	Any risks, including other risks not already discussed, that have the greatest potential for causing system failure. Include the effectiveness and use of the risk management plan.

Ask the Right People

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
- I/C security officer
- I/C and/or NIH 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 mitigation strategies and discuss mitigation 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 mitigation strategies for the most serious risks. If appropriate, assign risks to risk owners as described in the risk management plan.

APPENDIX C. TRACKING AND REPORTING RISK AND RISK MITIGATION

Risk management includes assessment of risk, development and execution of mitigation 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 mitigation activities.

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

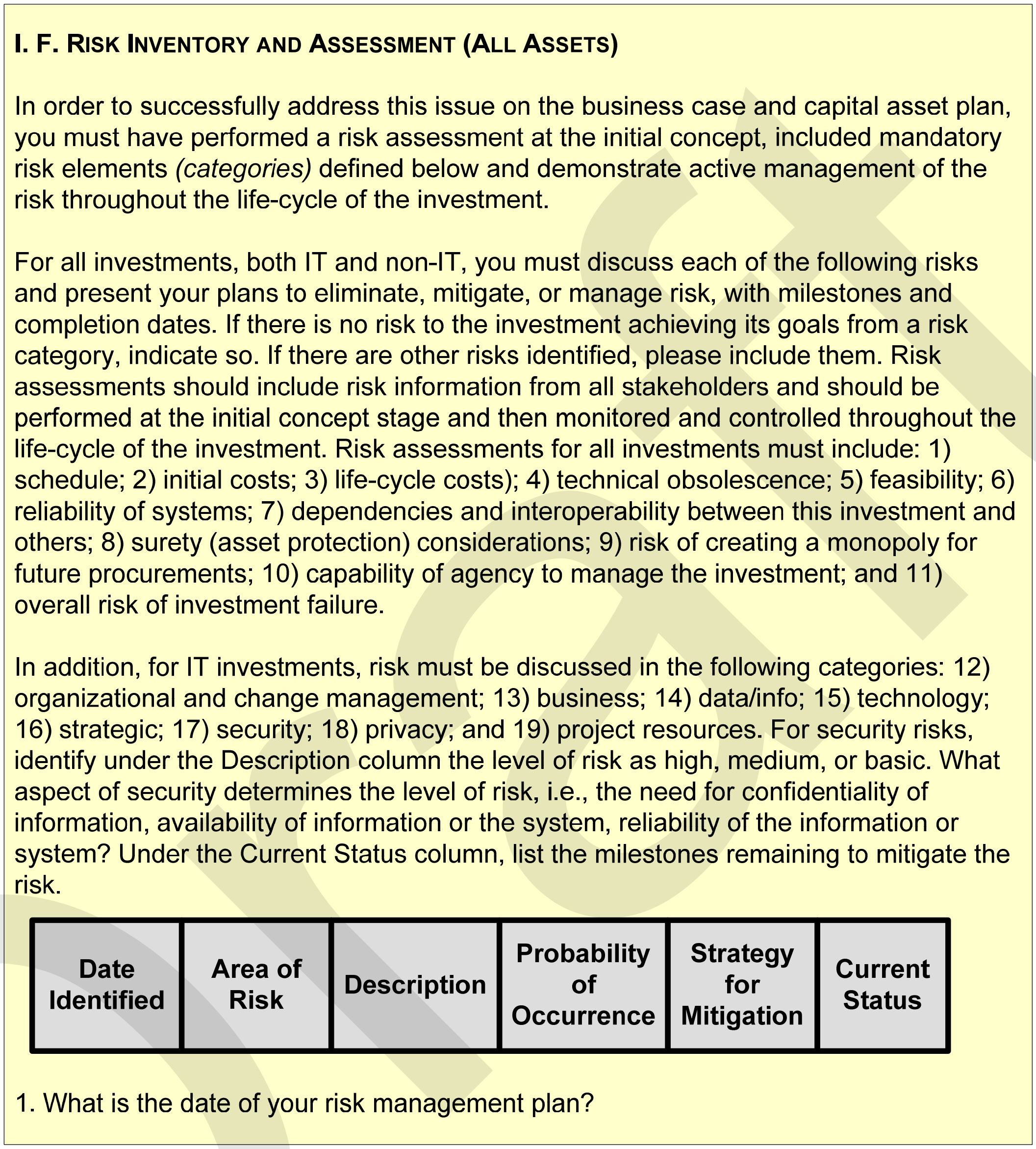
- *Tracking and reporting for internal project management, communication, and management of stakeholder expectations.* Appropriate reporting frequency and internal project team tracking and reporting procedures can be different for each project. Internal reporting procedures for your project should be 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 reporting formats presented in this appendix.

- *Tracking and reporting of risk management activities for external reporting to OMB or other oversight authorities.*

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, we believe that 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 C-1.

Figure C-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, 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 mitigation activities and when the risk will be mitigated.
- Proper formats for statements of risks and for risk mitigation strategies are included in the Risk Management Plan Template, Appendix A.
- If entering data into the ProSight portfolio management tool used by HHS to management its IT investments, 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 C-1 to evaluate and improve your reporting responses.

Table C-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say in the 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.	In Section I.F.1 (the Risk Plan section), 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.	In Section I.F.1, 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 C-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say in the 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.	In Section I.F.1, 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. In Section I.F.1, 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 system 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 C-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say in the 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 Section I.F, “Risk Inventory and Assessment,” paragraph 3, 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 (such as ProSight) 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 C-1. Check Sheet for Risk Management Compliance

Consideration	Reviewed	Advice	
		Corrective action	What to say in the 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 FY07, etc.). Be as specific as possible. In Section I.F.1, 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.