

# **NIH Risk Management Program**

## **Risk Management Guidebook:**

### **A Step-By-Step Guide**

**National Institutes of Health**  
Office of Management Assessment

**DRAFT**

June 2008

---

**DRAFT**



### Table of Contents

Purpose .....	3
Background .....	5
Introduction to Risk Management .....	7
The NIH Risk Management Organizational Framework .....	9
NIH Risk Management Roles & Responsibilities .....	10
The NIH Risk Management Methodology .....	15
1.0 Organize.....	17
2.0 Identify and Score .....	20
3.0 Assess.....	29
4.0 Remediate.....	35
5.0 Monitor .....	38
6.0 Report .....	40
Conclusion.....	41
Appendix A - List of Acronyms.....	42
Appendix B - Glossary of Terms.....	44
Appendix C - The Risk Capture Form.....	49
Appendix D - Corrective Action Plan (CAP) Template.....	57
Appendix E - Frequently Asked Questions.....	58
Appendix F - Reference.....	60



### Document Version Control

Version	Date of Issue	Brief Description of Change
1.0	May 02, 2008	N/A
1.1	May 27, 2008	Office of Management Assessment (OMA) consolidated comments incorporated into updated version.
1.2	June 10, 2008	Revisions to risk scoring incorporated into updated version.
1.3	June 17, 2008	Revisions to risk categories incorporated into updated version.



### Purpose

This **Risk Management Guidebook (Guidebook)** is a *detailed reference guide to carry out risk management activities at the National Institutes of Health (NIH)*. It includes an introduction to risk management principles and explains the value of risk management. The Guidebook provides a detailed explanation of each step in the NIH Risk Management Methodology, including guidance on how to perform each step.

The NIH Risk Management Guidebook is divided into the following sections and appendices.

#### **Section 1 - Background**

This section provides a brief background on the NIH risk management program and the factors that contributed to its development.

#### **Section 2 - Introduction to Risk Management**

This section provides the reader with a short introduction to risk management, defines risks and controls, and briefly discusses the value of risk management.

#### **Section 3 - The NIH Risk Management Organizational Framework**

This section discusses the NIH Risk Management Organizational Framework. This organizational segmentation is an arrangement of the agency to facilitate risk management activities.

#### **Section 4 - NIH Risk Management Roles and Responsibilities**

This section provides a description of NIH risk management roles and responsibilities.

#### **Section 5 - The NIH Risk Management Methodology**

This section describes the risk management methodology developed specifically for use at NIH. It consists of six distinct steps: Organize, Identify and Score, Assess, Remediate, Monitor, and Report.

#### **Section 6 - Organize**

Section 6 details the activities that make up the Organize step of the NIH Risk Management Methodology. The Organize step is an important initial step in beginning risk management activities at NIH.

#### **Section 7 - Identify and Score**

Section 7 discusses the activities that make up the Identify and Score step of the NIH Risk Management Methodology. Risk identification and scoring are fundamental activities in the methodology. This section instructs the reader on how to identify and score risks and what tools are available to assist in this process.

#### **Section 8 - Assess**

This section describes the activities that make up the Assess step of the NIH Risk Management Methodology. Assess involves conducting an analysis of the risks identified in the Identify and Score step.



### **Section 9 - Remediate**

Section 9 provides information about the activities that make up the Remediate step of the NIH Risk Management Methodology. The Remediate step consists of the activities required to address risks in order to reduce their impact or likelihood of occurrence.

### **Section 10 - Monitor**

This section describes the activities that make up the Monitor step of the NIH Risk Management Methodology.

### **Section 11 - Report**

Section 11 details the Report step of the NIH Risk Management Methodology.

### **Section 12 - Conclusion**

This section briefly concludes the primary portion of the NIH Risk Management Guidebook. Appendices containing additional reference information follow.

### **Appendix A - List of Acronyms**

Appendix A provides a listing of acronyms used throughout the NIH Risk Management Guidebook.

### **Appendix B - Glossary of Terms**

Appendix B contains a glossary of terms providing key definitions to terminology used throughout the document.

### **Appendix C - Risk Capture Form**

Appendix C provides a detailed description of each element of the Risk Capture Form tool that is used to identify and score risks. A copy of this form is also provided for reference.

### **Appendix D - Corrective Action Plan (CAP) Template**

Appendix D is a sample CAP template for reference.

### **Appendix E - Frequently Asked Questions**

Appendix E lists some frequently asked questions and provides answers to these questions.

### **Appendix F - Reference**

Appendix F includes web links to various resources such as the NIH risk management website.

### Background

In recent years, both the public and private sectors have placed a renewed emphasis on effective management practices. In 2004, the Office of Management and Budget (OMB) issued guidance for improving the management of operational, programmatic, and financial areas within government agencies. This guidance, issued under the authority of the Federal Managers Financial Integrity Act (FMFIA) of 1982, is designed to drive accountability and improve the efficiency and effectiveness of Federal programs.

In response to these requirements, and as part of an effort to improve the management of risk at NIH, an enterprise-wide Risk Management Program is being implemented. The **NIH Risk Management Program is an ongoing effort to perform standardized repeatable activities that promote the overall efficiency, effectiveness, accountability and integrity of the organization's work.** This program is supported by the NIH Steering Committee, and is designed to proactively identify and manage risks before they become obstacles to the NIH mission. In a memo sent to NIH employees, Dr. Zerhouni explained the importance and value of the Risk Management Program:



*"For us at NIH, effective risk management means enhancing our ability to ensure the overall efficiency, effectiveness, accountability, and integrity of our work. But risk management goes far beyond financial or administrative issues, it is also critical in ensuring sound science."*

Dr. Zerhouni tasked the NIH Office of Management Assessment (OMA) with developing the NIH Risk Management Program. In response to Dr. Zerhouni's tasking, OMA developed a program that allows for the implementation of a standardized risk management methodology that is designed to:

- Address both operational and management risks.<sup>1</sup>
- Identify risks and proactively manage them.
- Support the NIH research mission and vision.
- Provide a cross-cutting look at NIH risks.
- Provide senior leadership with consistent, prioritized risk information.
- Create an organized and integrated process of evaluating risks, including those that affect the entire agency.
- Improve strategic decision making.

At the onset of the program, the challenge was to establish an organizational framework and develop a risk management methodology that aligned with the NIH mission, culture, and

<sup>1</sup> This guidebook does not address financial risks that are covered under the OMB A-123 Appendix A.



organizational requirements. OMA focused on creating a methodology that can be consistently applied across NIH while maintaining sufficient flexibility to address the unique nature of each Institute and Center (IC) and Office of the Director (OD) Office. OMA obtained input from the NIH Senior Assessment Team (SAT) in an effort to establish a Program that meets the needs of the agency. The NIH Risk Management Organizational Framework and the NIH Risk Management Methodology are both discussed in further detail in the following sections of this Guidebook.

The NIH Risk Management Methodology was pilot tested at two organizations prior to the broad roll-out of the Program. The Office of Research Services (ORS) represented the OD during the pilot, while an IC perspective was provided by the National Institute of Allergy and Infectious Diseases (NIAID). These organizations implemented the first steps of the Risk Management Methodology and provided critical feedback to OMA on how to improve the methodology. The results of the pilot test were incorporated into the methodology and tools so that the Program can move forward to develop a Risk Baseline in the OD.

### Moving Forward

The next step for the NIH Risk Management Program involves working with staff within the OD to establish a **Risk Baseline**. ***A Risk Baseline is an enterprise-wide portfolio of risks that serves as a reference point for further risk management activities.*** A Risk Baseline will first be established in the OD.

**Risk Baseline:** The Risk Baseline is an enterprise-wide portfolio of risks.

As the primary policy-setting bodies at NIH, the offices that make up the OD are vital to the success of the Risk Management Program. The NIH Risk Management Program will first capture and address risks at the OD and later be rolled out to the various ICs. Once the Risk Baseline is established, OMA will communicate requirements for performing ongoing risk management activities.

The NIH Risk Management Program is based on six core principles.

- The Program will reinforce a culture of outstanding management.
- The NIH Risk Management Council (RMC) will oversee the Risk Management Program.
- All NIH managers have the responsibility to develop and maintain risk management programs.
- The scope of the program will include intramural, extramural, and IT processes, in addition to financial and administrative performance.
- A successful program requires proactive management that challenges the status quo.
- The program is of sufficient importance that resources must be devoted to assure its success.



### Introduction to Risk Management

Prior to a discussion of the NIH Risk Management Methodology, it is important to understand some of the basic principles of risk management. This section provides an introduction to the concepts of risks and controls with an explanation of the value and importance of risk management.

### Risk Management

**Risk management is a continuous process, carried out by the members of an organization, designed to proactively identify and mitigate risks to help promote the achievement of the organization's objectives, strategy, and mission.**

Risk management involves a process in which risks are identified throughout an organization so that appropriate actions can be taken to address them. Risk management also drives accountability by assigning responsibility to personnel for considering risk as a part of their daily jobs. Organizational silos are eliminated in an effort to promote awareness of risks that might be shared by more than one operating unit or division.

### What Is a Risk?

A **risk** is:

- An uncertain event or condition that may have a negative impact on an organization.
- Any event or condition that threatens the achievement of the objectives, goals, or mission of an organization.
- Uncertain because it has yet to occur.

### What Is a Control?

A **control** is:

- A mechanism to prevent or reduce the likelihood of a risk occurring.
- A means to reduce the impact of a risk should it occur.
- Designed to help promote the achievement of an organization's objectives, goals, and mission.
- Defined by organizational policies and procedures.
- A way to guide the daily activities of an organization and its employees.

Controls refer to the policies, procedures, or other processes that are designed to mitigate risks at an organization. Examples of controls at NIH include NIH Policy Manual Chapters, policies set at the HHS Department level, or requirements imposed on NIH by external third parties.



### The Value of Risk Management

Risk management is a value-added process that is incorporated into both the daily operational and strategic activities of an organization. By identifying risks and taking specific actions to prevent and mitigate them, an organization increases its operational effectiveness and its ability to accomplish the mission. Although it is not intended to be a strictly compliance-driven activity, risk management helps government organizations comply with regulations such as OMB Circular A-123 and FMFIA.

Risk management activities can allow an organization to:

- Identify barriers to success.
- Quantify risks using standardized criteria.
- Prioritize activities to focus resources where they have the greatest impact.

#### **Risk Management is not punitive.**

Risk management programs reward individuals who help the organization anticipate potential risks and who manage risks effectively to accomplish the mission while protecting resources.



# NIH Risk Management Guidebook

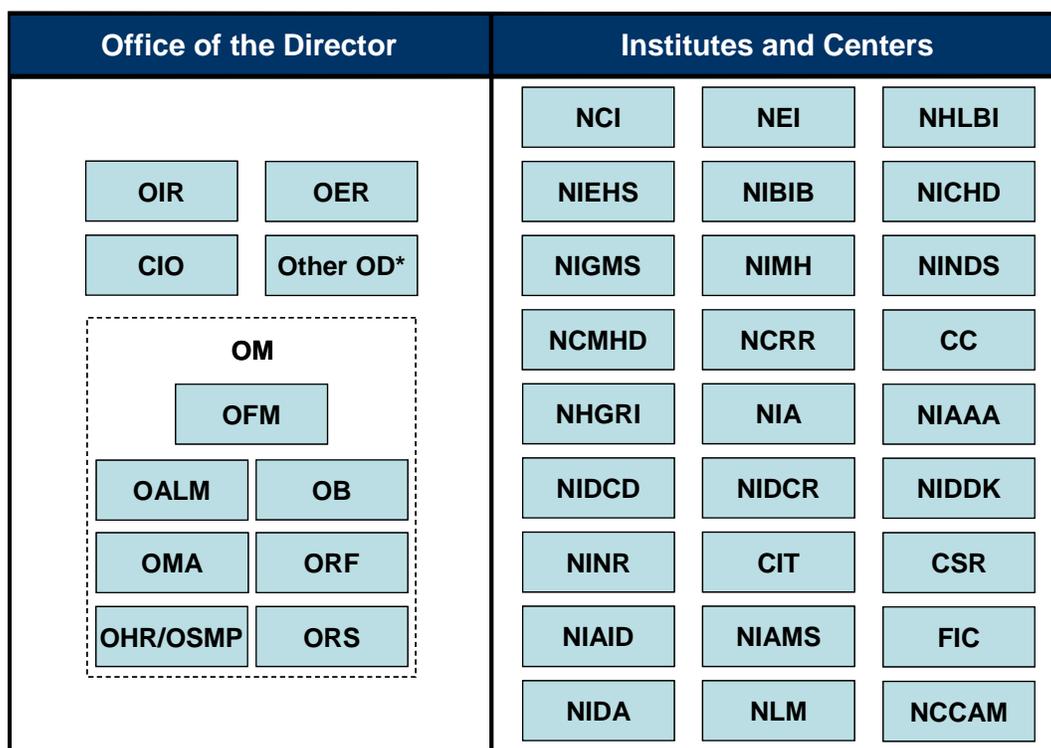
## The NIH Risk Management Organizational Framework

### The NIH Risk Management Organizational Framework

Prior to creating a methodology for managing risks at NIH, an organizational framework was defined. The NIH Risk Management Organizational Framework *is an arrangement of the agency to facilitate risk management activities at the enterprise level.*

The Framework involves dividing NIH into **Assessable Units (AUs)**. *An AU is a discrete mission oriented sub-set of an organization.* Although AUs are discrete organizations at NIH, the Risk Management Program encourages collaboration to manage risks that are shared across the agency.

At NIH, each of the 27 ICs is an AU. The OD is divided into an additional 11 AUs based on strategic groupings of certain offices. With the ICs and OD Offices combined, there are a total of 38 AUs at NIH. These AUs are displayed in the graphic below<sup>2</sup>.



\* Other OD includes: ORWH, OFACP, ES, OEODM, CCR, OLPA, OCPL, OSP, OPASI, NEO, ODP, OBSSR, OAR.

Figure 1

<sup>2</sup> Acronyms used in this graphic are defined in Appendix A



### NIH Risk Management Roles & Responsibilities

Certain individuals within the ICs and the OD Offices are assigned specific roles and responsibilities to carry out the NIH Risk Management Methodology. These individuals drive the success of the program by fulfilling their responsibilities and promoting a risk management culture within their organization. These roles and responsibilities are discussed in detail below.

#### NIH Director - Enterprise Risk Owner (ERO)

The NIH Director is the Enterprise Risk Owner (ERO). Although the NIH Director is not responsible for carrying out the remediation of specific risks, he or she takes ownership of the full set of risks facing the organization based on the responsibility to sign the annual FMFIA statement of assurance. With regard to risk management, the NIH Director:

- Signs the FMFIA statement of assurance for NIH.
- Fosters a risk management culture at NIH by providing sponsorship of the Risk Management Program and setting the "Tone at the Top."
- Holds NIH senior officials accountable for risk management through performance contracts.
- Examines data and risk management reports for trends in specific areas.
- Leads periodic meetings of the Risk Management Council (RMC).
- Sponsors the Risk Management Program through collaboration with OMA.

#### Steering Committee

The Steering Committee supports and advises the NIH Director. With regard to risk management, the Executive Steering Committee:

- Exercises stewardship over the use of NIH resources and provides oversight to promote programs that operate within established standards.
- Provides policy guidance and general oversight to support the successful completion of the yearly FMFIA statements of assurance.
- Provides recommendations to the NIH Director on required changes in policies, procedures, and resources to promote the successful operation of the NIH Risk Management Program.
- Provides a high-level summary of activities occurring within the Risk Management Council (RMC).

#### Risk Management Council (RMC)

The RMC is a grouping of NIH senior leaders, established to advise, support and provide a resource to the NIH Steering Committee on policies and procedures related to the NIH Risk Management Program. With regard to risk management, the RMC:

- Meets periodically to discuss risk management activities at their respective organizations in order to promote awareness of priority risks across the organization.
- Serves as a forum to discuss challenges in carrying out the NIH Risk Management Methodology within the AUs.
- Provides advice, recommendations, and helps shape the NIH Risk Management Program.
- Reports program status, key results, and policy issues quarterly to Principal Deputy Director.

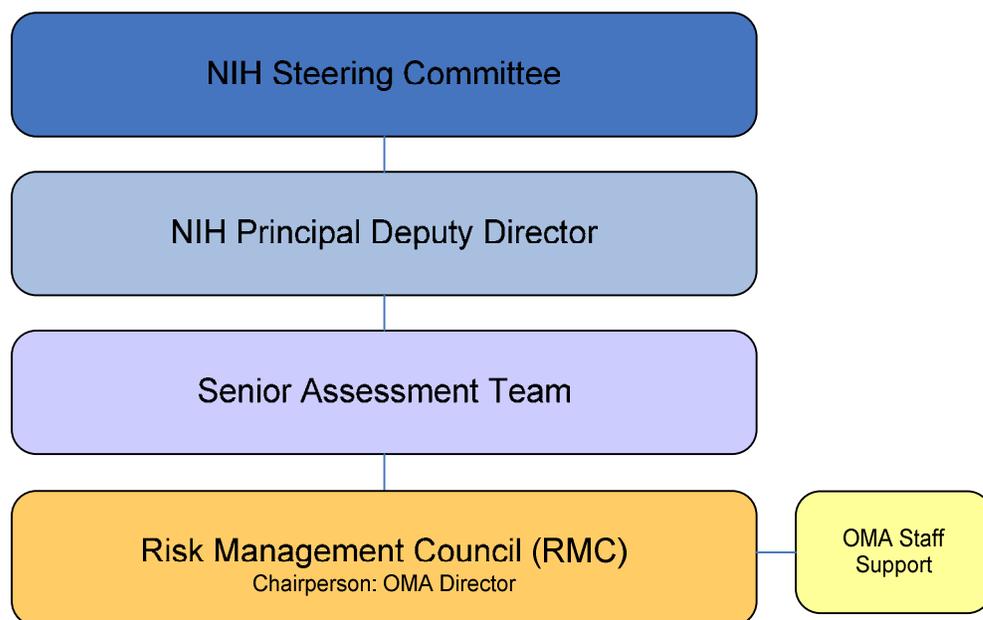


Figure 2

### Institute and Center (IC) Directors - Risk Owners (RO)

IC Directors serve as the Risk Owner for their AU. With regard to risk management, an IC Director:

- Is ultimately responsible for risks that are owned at the IC level.
- Oversees assessments of the adequacy of the NIH Risk Management Program and reinforces a climate of management excellence and integrity.
- Appoints the Risk Management Officer to conduct risk management activities.
- Supports the risk management activities of the Risk Management Officer and Risk Managers within the IC.
- Verifies annual FMFIA statement of assurance for accuracy and completeness.
- Signs and submits annual FMFIA statements of assurance to the NIH Director.

**Risk Owner (RO):**  
Owns all risks within an Assessable Unit.

### OD Office Directors - Risk Owners (RO)

OD Office Directors serve as the Risk Owner for their Assessable Unit. With regard to risk management, an OD Office Director:

- Is ultimately responsible for risks that are owned at the OD level.
- Oversees assessments of the adequacy of the NIH Enterprise Risk Management Program and reinforces a climate of management excellence and integrity.
- Appoints the Risk Management Officer to conduct risk management activities. (In some cases the RO may also be the RMO).
- Supports the risk management activities of the Risk Management Officer and Risk Managers within the OD Office.
- Verifies annual FMFIA statement of assurance for accuracy and completeness.
- Signs and submits annual FMFIA statements of assurance to the NIH Director (In most cases).



Figure 3

### Risk Management Officers (RMO)

Risk Management Officers are assigned by the IC Director or the OD Office Director. RMOs are designated as the responsible party for seeing that risk management activities within the AU are being conducted effectively. The RMO works closely with Risk Managers and reports directly to the IC Director or the OD Director. With regard to risk management, the RMO:

- Serves as the coordinating point for managing risk at the AU.
- Determines the risk management structure that is used to facilitate the risk management process within the Assessable Unit.
- Assigns Risk Managers (RMs) based on the risk management structure of the AU.
- Coordinates an effort with the RMs and other subject matter experts to validate the identified risks and controls.
- Works closely with OMA and consults with RMs on a regular basis.
- Reviews risks and submits to OMA for incorporation into NIH Risk Baseline.
- Reviews and approves Corrective Action Plans (CAPs) to determine whether the corrective actions provide a sufficient level of comfort that the risk has been managed.
- Coordinates with RMs to revise Corrective Action Plans if necessary.
- Monitors progress of CAPs and provides direct support to RMs to manage identified risks.



# NIH Risk Management Guidebook

## NIH Risk Management Roles & Responsibilities

- Approves and signs fully executed CAPs to signify completion and to provide reasonable assurance that the risk has been effectively managed.
- Provides documentation of executed CAPs to OMA as documentation of risk management activities in support of annual FMFIA statement of assurance.

### Risk Managers (RM)

Risk Managers (RMs) are selected based on the risk management structure at the AU. Risk Managers report to the RMO. With regard to risk management, the RMs:

- Execute responsibilities in compliance with applicable laws, regulations, and policies.
- Are responsible for identifying risks.
- Develop CAPs to address gaps and deficiencies in policies, procedures, and controls related to the identified risk and submit to RMO for approval.
- Execute actions as required by the CAP.
- Report the status of remediation activities to the RMO on a continuous basis.
- Inform senior management of possible problems.

### Office of Management Assessment (OMA)

OMA is responsible for developing a NIH-wide Risk Management Methodology, approach, tools, and procedures. OMA works with the ICs and the OD Offices to promulgate and assist with risk management activities. With regard to risk management, OMA:

- Communicates the NIH Risk Management Methodology to key stakeholders involved with the program.
- Develops relevant materials to illustrate the risk management process and articulates the importance of their active participation.
- Facilitates meetings with RMs to identify risks, applicable controls, policies and procedures, and demonstrates the specific stages of the risk management process.
- Aggregates results, analyzes results, and eliminates duplicate risks.
- Develops a Risk Heat Map that includes the identified risks for each AU.
- Communicates the output of the risk scores directly with RMOs.
- Provides guidance to RMs to develop and execute CAPs.
- Monitors NIH risk management activities.
- Conducts periodic quality reviews of risk management activities.
- Evaluates statements of assurance from each AU to present to the NIH Director.
- Prepares a summary report of corrective actions to present to the NIH Director in support of the NIH-wide statement of assurance.



### NIH Employees

NIH employees without a specific risk management role still have important responsibilities. One of the key goals of the Risk Management Program is to cultivate a risk management culture at NIH. This means that all employees should demonstrate an awareness of risk in their daily activities and proactively alert their supervisors when they come across risks. With regard to risk management, employees should:

- Comply with policies, procedures, and regulations related to their daily jobs.
- Demonstrate a willingness to elevate risks to management when necessary.
- Know who to contact with questions about the Risk Management Program.
- Promote a culture at NIH that embraces the identification of risks.

### The NIH Risk Management Methodology

A customized methodology was developed in order to deliver a risk management approach that specifically meets the needs of NIH. The **NIH Risk Management Methodology is a customized six step approach that provides a standardized means of addressing risks at NIH.** This methodology is shown in the graphic at the right.

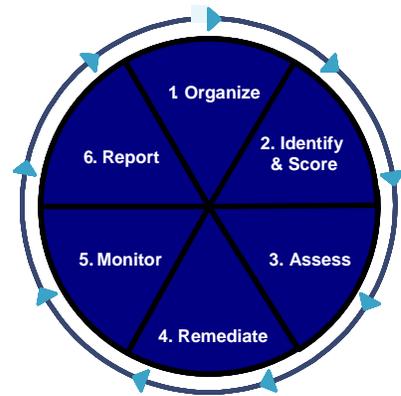


Figure 4

#### 1. Organize

Organize involves the following activities:

- Identifying RMOs
- Training RMOs
- Defining Risk Management Structures
- Identifying RMs
- Training RMs

#### 2. Identify and Score

Identify and Score involves the following activities:

- Identifying and Scoring Risks
- Reviewing Risks
- Providing Risk Information to OMA
- Validating Risk Information with OMA
- Establishing a Risk Baseline

#### 3. Assess

Assess involves the following activities:

- Determining Assessment Approach
- Assigning Responsibility for Assessment Activities
- Conducting Control Assessments

#### 4. Remediate

Remediate involves the following activities:

- Developing Corrective Action Plans (CAPs)
- Reviewing and Approving CAPs
- Executing CAPs
- Reviewing Executed CAPs

### 5. Monitor

Monitor involves the following activities:

- Monitoring the Risk Baseline

### 6. Report

Report involves the following activities:

- Reporting

Each of these six risk management steps and their associated activities are outlined in the Work Breakdown Structure (WBS) found below. These activities are discussed in detail in the following sections of this document.

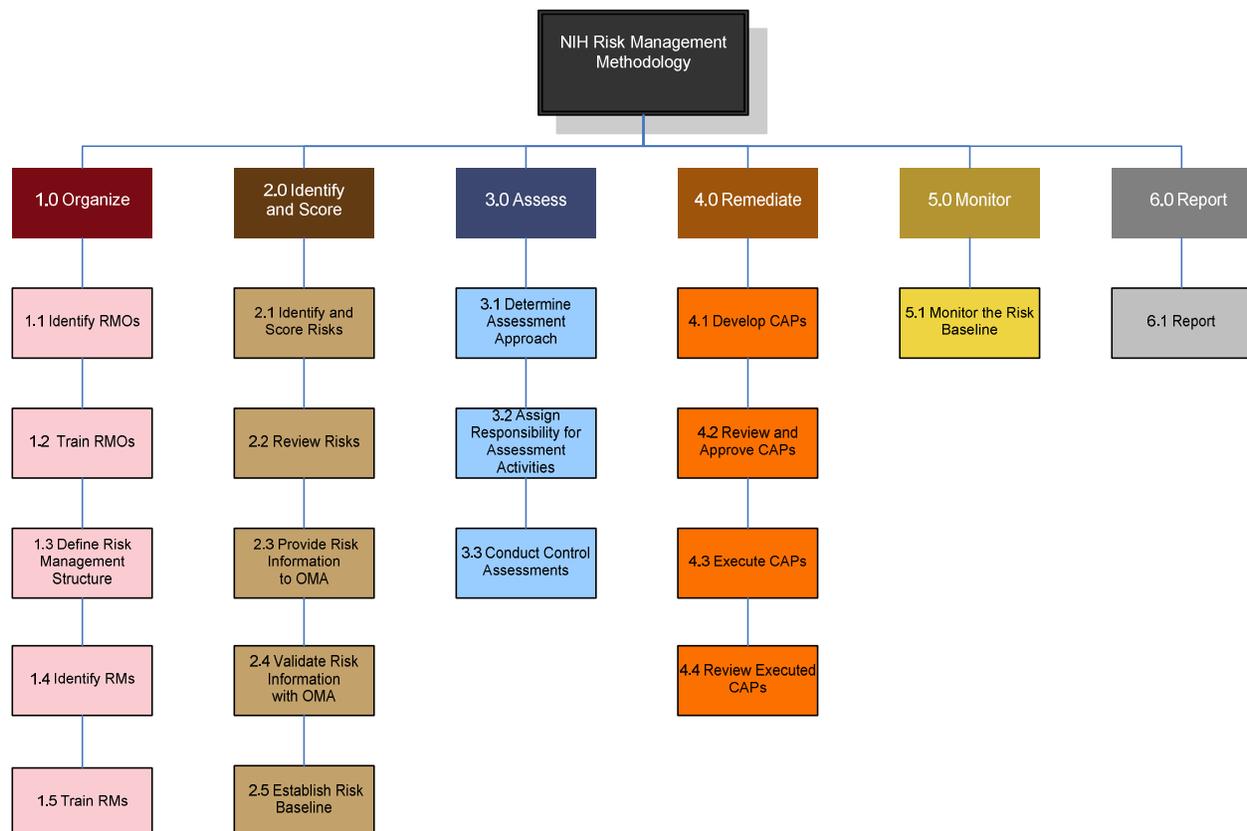


Figure 5

### 1.0 Organize

The Organize step consists of five major activities that prepare an AU to carry out the NIH Risk Management Methodology. Before identifying, scoring, assessing, and remediating risks, personnel with key roles and responsibilities for the Risk Management Program are identified within each AU. These personnel are responsible for defining a structure within the organization in order to establish clear lines of authority.



Certain aspects of the Organize step are one-time activities that do not need to be repeated annually. Once an AU completes the necessary activities, the Organize step only needs to be revisited when significant changes occur within the AU, such as a change in key personnel or reorganization. The key activities of the Organize step are depicted below.



#### 1.1 Identify RMOs

The first activity in the Organize step is to appoint an RMO within each AU. The RMO has a number of important responsibilities in the NIH Risk Management Program, so identifying this person is a critical step. The RMO is usually the Executive Officer of an IC or the Director of an OD Office. RMOs are identified by senior management in coordination with the Office of Management (OM) and OMA.

It is not necessary to appoint a new RMO on an annual basis. However, when an existing RMO leaves the organization or assumes a different position, he or she must be replaced and the change must be communicated immediately to OMA. The RMO serves an important coordinating role for risk management activities within an AU, so it is critical to staff this position at all times.

**Risk Management Officer (RMO):**  
Coordinates risk management activities at the AU level.

#### 1.2 Train RMOs

OMA provides role-based training to RMOs to educate them on their specific responsibilities. This training provides an introduction risk management, including a discussion of risks and controls. Once the RMOs have a basic understanding of risk management, the training gives more detailed instructions on executing the NIH Risk Management Methodology within an AU. Lastly, the training provides guidance on how to define the risk management structure within an AU.

## 1.3 Define the Risk Management Structure

After RMOs have received initial training, they are tasked with defining the **risk management structure** for their AU. **A risk management structure is a segmentation of an AU to facilitate risk management activities at the AU level.** A risk management structure allows the divisions, offices, and functions within an AU to be involved in the risk management process. The structure also allows organizations to clearly assign ownership of risks to the appropriate personnel.

Due to the unique nature of each IC and OD Office, the RMO has the flexibility to define the risk management structure in the manner that is most appropriate for his or her organization. If the RMO can leverage a pre-existing management group that has representatives from different areas within the AU, then this may prove to be the most efficient and natural way to define the risk management structure. If the AU does not have a pre-existing management group, then there are two suggested approaches to defining the risk management structure:

**Risk Management Organizational Framework:** An arrangement of the agency to facilitate risk management activities at the enterprise level. (Refer to page 9 for more detail).

**Risk Management Structure:** A segmentation of an AU to facilitate risk management activities at the AU level.

1. The organizational approach
2. The functional approach

## Sample Risk Management Structures: Organizational Approach

The organizational approach relies on the pre-existing organizational chart of the AU. Each office and division is responsible for conducting risk management activities and reporting to the RMO. A sample organizational risk management structure is shown below for the Office of Research Services (ORS). Please note that this graphic is for notional purposes only.

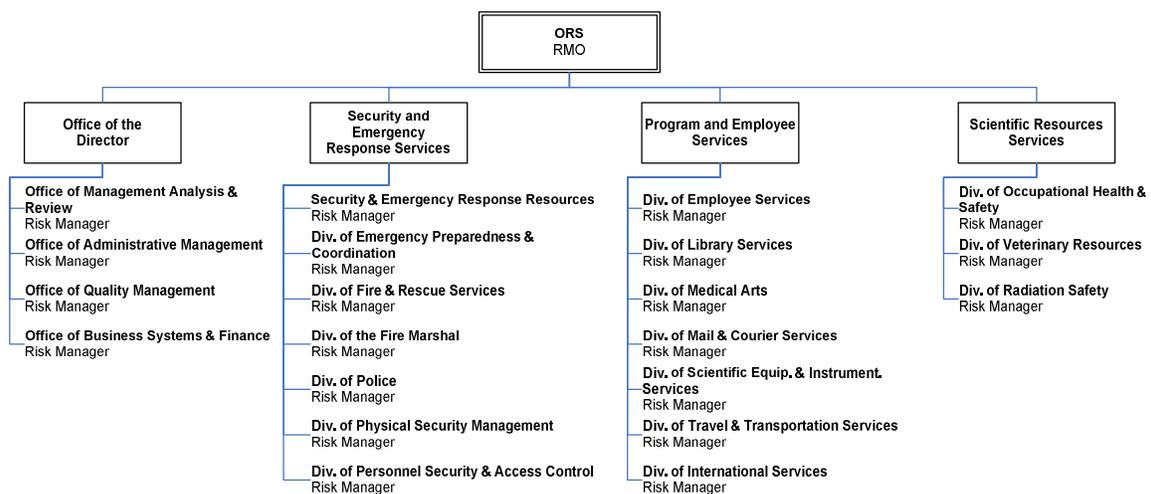


Figure 6

## Sample Risk Management Structures: Functional Approach

The functional approach breaks down the AU according to primary business functions rather than divisions and offices. A sample functional risk management structure is shown below for the National Institute of Allergy and Infectious Diseases (NIAID). Please note that this graphic is for notional purposes only.

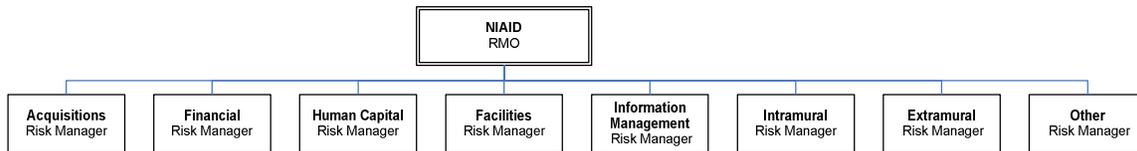


Figure 7

### 1.4 Identify RMs

The RMO identifies RMs according to the risk management structure of the AU. If the organizational approach is used, the RMs are senior managers at the division or office level. If the functional approach is used, the RMs are senior managers within each functional area.

Personnel serving as RMs are in a management position with a strong understanding of the potential risks that face his or her area of the AU. It is important for the RM to work with the RMO and other employees at the AU to support the risk management process.

**Risk Manager (RM):**  
Responsible for identifying risks and taking actions to mitigate risks.

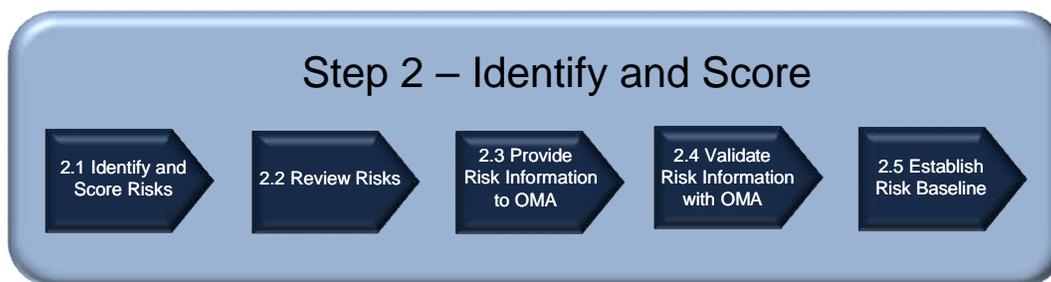
RMs work closely with the RMO to carry out risk management activities in the AU. As a result, RMOs should make every effort not to identify too many RMs because doing so may complicate communication and risk management activities.

### 1.5 Train RMs

OMA provides training to the RMs that are identified by the RMO. Similar to the RMO training, this training discusses the basics of risk management, including a discussion of risk and controls with an introduction to the NIH Risk Management Methodology. Due to the specific roles and responsibilities of RMs, the training focuses on the risk identification and scoring step of the methodology.

### 2.0 Identify and Score

Risk identification and scoring are fundamental activities in the risk management methodology. Risk identification begins with personnel from the organization's risk management structure identifying and scoring risks. These risks are reviewed and then provided to OMA. Before establishing the risk baseline for the organization, OMA meets with RMOs and RMs to validate the risks that have been identified. The Identify and Score step consists of five major activities as depicted below.



#### 2.1 Identify and Score Risks

The first activity that takes place during the Identify and Score step is to identify and score risks affecting the AU or NIH as a whole. Based on guidance provided by OMA, the RMO and RMs work closely to identify and score risks in their respective areas.

#### Developing a Risk Statement

The first step in identifying a risk is to develop a **Risk Statement**. **A risk statement is a detailed description of a potential risk and its perceived effect.** Risk statements are crafted by using an "if-then" statement. By focusing on phrasing risk statements this way, a standardized approach is brought to the process.

The "if" portion of the risk statement relates to an uncertain event or condition that may occur. The "then" portion of the risk statement describes the potential outcome of the risk. An example of a very simple risk statement is included below:

**"If** I sleep too late, **then** I will be late for work."

Examples that are more specific to the NIH environment include the following risk statements.

**"If** patient samples from clinical studies are not stored and identified properly, **then** we will not be able to analyze data properly or comply with federal rules for biospecimen inventories."

**"If** fire safety training is not provided to required health care staff in accordance with the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) requirements, **then** NIH could realize a compromised level of safety for patients and



visitors to the Clinical Center; JCAHO accreditation could be jeopardized; and the NIH could be subject to negative publicity.

When constructing the "if-then" statement, individuals should:

- **Think strategically.** Consider the goals, objectives, and mission of the organization. Any event or condition that could prevent or inhibit the accomplishment of the organization's goals, objectives, or mission should be documented as a risk.
- **Think about materiality.** Identify risks that have a legitimate and material effect on the organization. Identified risks should be related to the operations of the organization, and they should have potential negative effects that are more than negligible.
- **Think about cause-and-effect relationships.** The occurrence of an event or the presence of a condition could have certain implications for NIH. Consider the types of events or conditions (causes) whose occurrence would have a legitimate negative impact (effect) on the agency, and formulate your "if-then" statement accordingly. Some causes may have multiple effects. These should be articulated to promote a full understanding of the risk.

### Capturing Risks Using Standardized Tools

NIH uses a **Risk Capture Form** to identify and score risks. *The Risk Capture Form is a standardized data entry tool for capturing risk information.* It brings consistency to the process of identifying and scoring risks across the agency. Without standardized tools, risk data would vary greatly from one AU to another. The Risk Capture Form requires RMs to phrase their risk statements using the "if-then" approach to promote consistency across NIH. The Form also requires the completion of a number of other standardized questions designed to capture important risk information.

The first section of the Risk Capture Form contains a series of fields that must be completed for each identified risk. The second section of the Form contains a series of questions that derive a risk score. The following guidance discusses the key elements of the Risk Capture Form and provides a standardized practice for risk identification and scoring.

The screenshot shows the NIH Risk Capture Form interface. It is divided into several sections:

- User Information:** Fields for Name, Date (month/day/yy), Position/Title, Accessible Unit, Division/Office, Email Address, and Telephone Number.
- Risk Statement:** A section for writing an "if-then" statement for the risk.
- Risk Information:** Fields for Immediate, Span of Control, Risk Category, and a question about primary policies, procedures, and controls.
- Risk Impact:** Questions about the impact on the NIH Mission, Public Trust, Organizational Impact, and Financial Impact.
- Risk Likelihood:** Questions about professional judgment, written policies/procedures/controls, awareness of the risk, and management actions.

Figure 8

The Risk Capture Form has several non-required fields. If any information is known, RMs should make every effort to provide it in order to increase the quality of the risk information. Detailed guidance for completing the Risk Capture Form can be found in Appendix C of this document.



### Scoring Risks

Two factors are considered when scoring risks:

- Impact
- Likelihood

**NO classified material** should be addressed as part of the risk identification exercise.

***Risk Impact is the potential effect that a risk may have.***

***Risk Likelihood represents the chance that a risk may occur.***

At NIH the score for each of these factors is calculated based on responses to a set of questions contained in the Risk Capture Form. Individuals respond to these questions for each identified risk in order to arrive at a risk impact score and a risk likelihood score. The sum of the impact and likelihood scores determines the overall risk score.

### Impact

At NIH, Risk Impact is quantified by assigning a numerical score based on responses to a series of questions on the Risk Capture Form. Impact is scored based on the following five dimensions:

- Mission Impact
- Impact on Public Trust
- Organizational Impact
- Financial Impact
- Professional Judgment

Using the Risk Capture Form, individuals respond to the five questions in the table below to indicate the impact of the risk. Their responses result in the calculation of an Impact score.

		Impact Questions	Responses to Impact Questions		
Weightings	20%	What is the Impact on the NIH Mission?	The risk could have a minimal effect on the NIH Mission.	The risk could have a significant effect on the NIH mission.	The risk could have a severe effect on the NIH mission.
	20%	What is the Impact on Public Trust?	The risk could have a minimal effect on the Public Trust.	The risk could have a significant effect on the Public Trust.	The risk could have a severe effect on the Public Trust.
	20%	What is the Organizational Impact?	The risk could affect a single office, department, or division.	The risk could affect more than one OD Office or IC.	The risk could affect all of NIH or extend beyond NIH.
	20%	What is the Financial Impact?	The risk could result in a Financial Impact of up to \$500,000.	The risk could result in a Financial Impact ranging between \$500,000 and \$5 million.	The risk could result in a Financial Impact greater than \$5 million.
	20%	What is the overall Impact based on your Professional Judgment?	In my Professional Judgment, the risk could have a minimal overall impact on the NIH.	In my Professional Judgment, the risk could have a significant overall impact on the NIH.	In my Professional Judgment, the risk could have a severe overall impact on the NIH.

Figure 9



### Mission Impact

- Mission Impact is based on the potential impact of the risk on the NIH mission.
- The Mission Impact considers the fact that a risk could negatively impact the achievement of the strategic goals and objectives that make up the NIH mission.
- Responses to this question include:
  - a) The risk could have a minimal effect on the NIH mission.
  - b) The risk could have a significant effect on the NIH mission.
  - c) The risk could have a severe effect on the NIH mission.

### Impact on Public Trust

- Public Trust refers to the level of confidence that individuals or groups outside of NIH have in the agency. Individuals or groups may include patients, patient advocates, the research community, Congress, the Administration, and the American public.
- Public Trust risks impact the reputation of NIH.
- Responses to this question include:
  - a) The risk could have a minimal effect on the public trust.
  - b) The risk could have a significant effect on the public trust.
  - c) The risk could have a severe effect on the public trust.

### Organizational Impact

- Organizational Impact refers to how broadly the risk affects NIH.
- Responses to this question include:
  - a) The risk could affect a single office, department, or division.
  - b) The risk could affect more than one OD Office or IC.
  - c) The risk could affect all of NIH or extends beyond NIH.

### Financial Impact

- Financial Impact captures the approximate cost to the organization if the risk was realized.
- Use of Financial Impact scoring allows for a quantitative element to be integrated into the methodology.
- Responses to this question include:
  - a) The risk could result in a financial impact of up to \$500,000.
  - b) The risk could result in a financial impact ranging between \$500,000 and \$5 million.
  - c) The risk could result in a financial impact greater than \$5 million.

### Professional Judgment

- Professional Judgment is included to provide risk identifiers with a means of indicating the perceived impact of a risk based on their own experiences and evaluation of the risk.
- Responses to this question include:
  - a) In my professional judgment, the risk could have a minimal overall impact on the NIH.
  - b) In my professional judgment, the risk could have a significant overall impact on the NIH.
  - c) In my professional judgment, the risk could have a severe overall impact on the NIH.

### Likelihood

Likelihood is scored based on responses to six questions. Individuals use the Risk Capture Form to respond to the questions in the table below. Their responses result in the calculation of a Likelihood score.

		Likelihood Questions	Responses to Likelihood Questions			
Weightings	40%	Are written policies, procedures, or controls in place to manage this risk?	Yes		No	
		Written policies, procedures, or controls are effective (if applicable).	Strongly Agree	Agree	Disagree	Strongly Disagree
		Are all policies included as Manual Chapters in the NIH policy manual?	Yes		No	
	20%	Individuals within my organization are aware of this risk.	Strongly Agree	Agree	Disagree	Strongly Disagree
	20%	Is management taking formal actions to mitigate or address this risk?	Yes		No	
	20%	In your professional judgment, what is the likelihood that the identified risk could occur?	Very Unlikely	Unlikely	Likely	Very Likely

Figure 10

### Are written policies, procedures, or controls in place to manage this risk?

- This question identifies whether or not written policies, procedures or controls are in place to manage the risk.
- The likelihood of the risk being realized is greater if policies, procedures, or controls are not in place.
- Responses to this question include:
  - a) Yes.
  - b) No.

Examples of policies, procedures, and controls include NIH Policy Manual chapters, or any other documented processes that are followed related to this risk.



### **Written policies, procedures, or controls are effective (if applicable).**

- This question is contingent on the response to the first likelihood question. If the first likelihood question is answered "no", this likelihood question does not apply.
- This question asks the identifier to indicate how well they feel written policies, procedures, or controls are working.
- Responses to this statement include:
  - a) Strongly Agree.
  - b) Agree.
  - c) Disagree.
  - d) Strongly Disagree.

### **Are all policies included as Manual Chapters in the NIH policy manual?**

- This question is contingent on the response to the first likelihood question. If the previous question is answered "no", this likelihood question does not apply.
- Responses to this question include:
  - a) Yes.
  - b) No.

### **Individuals within my organization (Assessable Unit) are aware of this risk.**

- This question addresses the overall level of awareness of the risk in the organization.
- Individuals should consider whether awareness of the risk is limited to a small group of people, or is there widespread awareness of this risk throughout the organization?
- Responses to this statement include:
  - a) Strongly Agree.
  - b) Agree.
  - c) Disagree.
  - d) Strongly Disagree.

### **Is management taking formal actions to mitigate or address this risk?**

- This question asks if management is doing anything currently to address the risk.
- Formal actions include sponsoring training and education programs, redesigning the existing process, conducting a management review, or other similar activities.
- Responses to this question include:
  - a) Yes.
  - b) No.

In your professional judgment, what is the likelihood that the identified risk could occur?

- This question allows the individual a means of indicating the perceived likelihood of a risk occurring based on their own experiences and evaluation of the risk.
- Responses to this question include:
  - a) Very Unlikely.
  - b) Unlikely.
  - c) Likely.
  - d) Very Likely.

### Risk Scores

A **Risk Score** is the sum of the points assigned to an individual risk based on the responses to the impact and likelihood questions on the Risk Capture Form. Risk Scores allow for quantitative comparison and ranking of risks across NIH. Based on the responses provided for impact and likelihood questions a numeric score is assigned along with a corresponding color (Red, Yellow, Green) for both impact and likelihood. The point value assigned to the individual questions is not provided in the form or this document to avoid promoting bias. Using the scores, risks can be plotted on a risk heat map (as discussed later).

**Risk Impact:** The potential effect that a risk may have.

**Risk Likelihood:** The chance that a risk may occur.

### 2.2 Review Risks

After risks have been identified and scored within the AU, the RMO reviews the risks. It is recommended that the RMO conducts a meeting with RMs and other staff to discuss the identified risks. During the meeting, the RMO and RMs collectively evaluate the identified risks and the associated scores. This process helps to reduce bias in the scoring, and leads to increased risk quality. The RMO and RMs also benefit from having an open discussion about the risks facing the organization due to the increased level of awareness throughout the AU that such a meeting provides.

If it is not feasible to conduct a group meeting, RMs submit their risks to the RMO. The RMO coordinates activities between RMs and subject matter experts to review risks and determine if they have been appropriately scored.

### 2.3 Provide Risk Information to OMA

Once the risks are reviewed, the data is submitted to OMA by the RMO. OMA organizes the risk data from the AU and creates a **Risk Heat Map** based on the results of scoring. OMA also maintains a master Risk Heat Map that provides an enterprise perspective of risks at NIH.

### The Risk Heat Map

A Risk Heat Map is a graphical representation of identified risks. It is a tool used to show the magnitude of a risk measured in terms of Impact and Likelihood. The Risk Heat Map is a graph where risks are plotted according to their Impact score along the X-Axis and according to their Likelihood score along the Y-Axis. The resulting point that is plotted on the Risk Heat Map can be used to observe the relative influence of the risk compared to other plotted risks. Using a Risk Heat Map, the organization can quickly see what risks may require the greatest or most immediate attention. Individuals within the AUs do not need to perform any additional work to develop an aggregate listing of risks or a risk heat map. OMA provides this information to the AUs once it has been compiled.

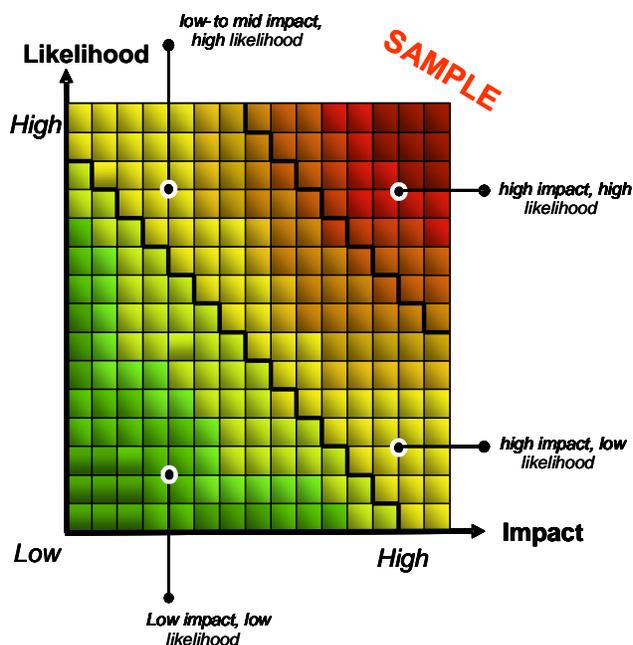


Figure 11

### 2.4 Validate Risk Information with OMA

After risks have been reviewed by the RMO and provided to OMA for their initial analysis, the identified risks are validated. **Risk validation is a process in which risk data is reviewed, discussed, and clarified in order to gain a thorough understanding of the risk before it is finalized.** OMA works with key personnel from the AUs to make certain that all information is accurate and complete, clarify risk statements, eliminate duplicate risks, and discuss the risk scores. This process enhances the overall quality of risk information and is essential to support later steps in the Risk Management Methodology.



### 2.5 Establish a Risk Baseline

After completing validation activities, OMA compiles risk data to establish the Risk Baseline, which is a list of risks that serves as a starting point for further risk management activities. It is expected that the baseline will change over time as new risks are introduced into the NIH environment and others become obsolete.

### 3.0 Assess

The purpose of the Assess step is to evaluate the processes and controls associated with each risk. The evaluation of the processes and controls is structured using a tiered approach designed to help NIH focus its resources on its most significant risks. The outcomes of the Assess step support remediation efforts. The Assess step involves the following three activities. Each is explained in the following sections.



#### 3.1 Determine Assessment Approach

The first activity in the Assess step involves an analysis of risks based on where they are plotted on the Risk Heat Map. The aggregate risk score determines whether risks are categorized as high, medium, or low, which equates to the Red, Yellow, and Green areas on the Risk Heat Map. This categorization leads to the NIH **Tiered Risk Assessment Approach**. *The tiered risk assessment approach dictates the requirements for assessing risks based on their severity.* The following guidelines form the basis of this tiered approach.

Risk Scoring Results	Level of Assessment	Assessment Description
Red Risks	Tier One	Red risks require documentation of relevant controls and processes. Control tests are conducted to determine the effectiveness of controls.
Yellow Risks	Tier Two	Yellow risks require documentation of relevant controls and processes. A process analysis is conducted to identify control gaps and deficiencies.
Green Risks	Tier Three	Green risks do not require documentation of relevant controls or processes. No control testing or process analysis is required.

Figure 12



### 3.2 Assign Responsibility for Assessment Activities

During the Risk Identification and Scoring step, it is possible to identify risks specific to an individual AU or risks that may cross multiple AUs. In either case, it is necessary to clearly define "ownership" of each risk and assign responsibility for the activities of the Assess step.

***A Risk Owner is the individual who has the authority to manage risks and/or controls within an AU. The RO responsibility is assigned to IC directors and OD office directors.***

The scope of the risk is used to determine risk ownership.

**1. Risks Localized Within an AU.** A risk may have the potential to occur only within a single AU. For example, a risk related to the Vaccine Research Center might only apply to NIAID. Therefore, the NIAID director would serve as the risk owner.

While it is most likely that a risk related to the Vaccine Research Center would be identified by NIAID, there is a possibility that the risk might be identified by another AU. In either case, the NIAID director would still serve as the risk owner because the NIAID director has the responsibility for and authority over the Vaccine Research Center.

**2. Cross-AU Risks.** In other instances, a risk may have the potential to occur across multiple AUs. In these cases, an owner must be selected from the multiple AUs to lead the Assess step and coordinate downstream activities related to remediation, monitoring and reporting. OMA will identify cross-AU risks within the Risk Baseline and will identify a risk owner.

For many cross-AU risks, it is likely that authority for the related controls will reside within an OD office. For example, a risk related to intramural research performed by multiple ICs would be governed by the policies and controls set forth by the OD Office of Intramural Research. In this instance, risk ownership would be assigned to the Director of the Office of Intramural Research.

Once ownership is assigned, responsibility for Assess activities (and for the later steps of Monitor and Report) may be delegated within the risk owner's AU. Delegation for these responsibilities may reside with the RMO or a Risk Manager who is empowered to successfully execute the Assess activities.

The tier structure and the risk ownership are also used to determine how Assess activities are supported. Assess activities for localized risks should be managed within the individual AU by the AU. OMA will support Assess activities for cross-AU Tier 1 red risks.

### 3.3 Conduct Control Assessments

The tiered approach requires a controls assessment for Red and Yellow risks, and no controls assessment for Green risks. The assessment of Red risks involves control testing, but Yellow risks do not require control testing. The following sections provide detailed descriptions of assessment activities according to the tiered approach.

## Tier One Controls Assessment - Red Risks

The following steps detail the activities associated with a Tier One controls assessment. These steps assume that responsibility for the activities has been delegated to a RM.

### 1. Identify Process Owners

The RM develops a list of individuals who have control over the policies, procedures, and controls related to the risk.

### 2. Define Assessment Team

The RM establishes a team of personnel to conduct the assessment. Team members may include process owners, management analysts, contractors, or other resources available at the AU. These individuals should have knowledge of the processes related to the specific risk and should have experience with the assessment activities.

### 3. Document Processes and Controls

The team identifies the related policies, procedures, and controls. When these are unavailable, the team will need to document policies, procedures and controls. This activity results in the development of process map documentation. The process maps provide details of activities, tasks, responsibilities, and key decision points in a given process. The purpose of process mapping is to identify control points in the process and the control activities performed by users. A sample process map is shown at right.

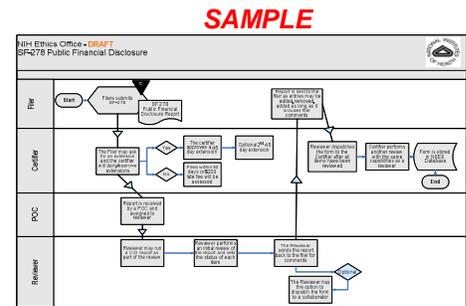


Figure 13

### 4. Conduct a Process Analysis

Once the documentation is available, the RM analyzes the information to help determine if there are adequate controls in place and if the controls are designed effectively. The analysis includes the identification of key controls to be tested.

### 5. Develop Test Plan Matrices and Test Plans

The RM develops Test Plan Matrices to document the key controls with the corresponding risks. A Test Plan Matrix contains the relevant information for each documented process. A sample Test Plan Matrix is provided below.

SAMPLE

Risk and Control Data					Control Testing Activity					Design Assessment			
Control Reference Number	Control Objective	Risk Focus Area	Control Activity	Process Owner (name, title, division)	Manual (M) or Automated (A)	Application (if Automated)	Frequency of Control	Testing Period	Population and Sample Size	Testing Method	Evidence of Control	Design Gap	Comments
NEO.4.N8	Validate that staff who are required to file SF 278 are compliant	a. Participate in a matter where they have a personal or imputed financial interest b. Holding a financial interest prohibiting by HHS regulation	NIH employees in certain pay plans or positions are required to file a Public Financial Disclosure (SF 278) within 30 days of entering a covered position and within 30 days of terminating from a covered position. Each SF 278 must be certified by the DEC.		M	n/a	Continuous	FY 07 through current	45	Random Sampling	SF 278/NEES Screenshots		

Figure 14



Test Plans are created to facilitate tests of controls. Test Plans include descriptions of the attributes that will be tested in relation to the key controls. A sample Test Plan is provided below.

NIH Conflicts of Risk Assessment							
Red Risk Control Testing Matrix - NIH Ethics Office							
<b>SAMPLE</b>							
Reference Number	NEO.4.X						
Control Activity	NIH employees in certain pay plans or positions are required to file a Public Financial Disclosure (SF 278) within 30 days of entering a covered position and within 30 days of terminating from a covered position. Each SF 278 must be authorized by the DEC.						
Criteria for Effectiveness	No tolerance for errors, all exceptions are reported.						
Control Frequency	Continuous						
Population Definition	List of NIH individuals who meet these criteria: SES, ST, or SL pay plans, Commissioned Officers at or above the O-7 rank, the four NIH level Deputy Directors (NIH DD, DDM, DDER, DDIR), all IC Directors, Deputy Directors, Clinical Directors, and Scientific Directors, and others as set forth in the EIGA.						
Sample Size	45						
Test Results							
Number of Deviations							
Findings and Conclusion							
Sampling Procedure Performed	Take a random sample of NIH employees who are required to file SF 278 and reconcile in the NEES database to determine compliance (Pre-clearance, Filed annually, new entrants, people terminating) (Annual and new entrants should be included)						
Control Attribute Description:							
<ul style="list-style-type: none"> <li>A. Obtain population sample that meets criteria</li> <li>B. Look up date stamp to ensure form was completed in the appropriate time (60 day review)</li> <li>C. If individual completes after deadline, ensure there is an extension approval attachment</li> <li>D. Ensure that individual has completed form from database accurately with DEC signature</li> </ul>							
Sample Number	Sample Identification			Control Attribute A	Control Attribute B	Control Attribute C	Control Attribute D
	Sample Name	Date	NEES				
1							
2							
3							

Figure 15

## 6. Obtain Samples and Conduct Tests of Controls

The RM obtains samples from process owners within the appropriate AU. Samples provide evidence of sign-off approvals, authorizations, trainings, or other control objectives. These samples serve as the basis for conducting tests to determine the effectiveness of controls. If a sample does not show evidence that the control was properly executed, then it is noted as an exception (e.g., a document that lacks proper authorization is noted as an exception). The Implementation Guide for OMB Circular A-123 provides guidance on the number of samples required for testing based on the frequency of the control being tested, as shown at right<sup>3</sup>. This guidance is used by NIH in most cases. However, in some instances it may be determined that larger sample sizes are required in order to obtain better results.

Control Frequency	Sample Size
Annually	1
Semi-Annual	2
Quarterly	2
Monthly	3
Weekly	10
Daily	30
Continuous	45

Figure 16

Testing results are recorded on Test Plans. A summary of testing results is added to the Test Matrix. The results of control tests serve as the basis for the Remediate step of the methodology, which is explained in the Remediate section of the Guidebook.

<sup>3</sup> Implementation Guide for OMB Circular A-123, Page 36.



Controls testing can have the following results that require certain actions during remediation.

- **Control Gap** - A control gap requires the implementation of a control in an area that previously lacked an appropriate control. An example would be drafting a policy to address an area that previously lacked guidance or a formal process.
- **Operating Deficiency** - An operating deficiency exists when a properly designed control does not operate as intended, or when the person performing the control does not possess the necessary authority or qualification to perform the control effectively.
- **Design Deficiency** - A design deficiency exists when a control is not properly designed. For this type of deficiency, even if the control operates as designed, the control objective is not always met.
- **No Weakness** - After completing testing it may be determined that adequate controls are in place and operating effectively. Despite this, the risk may still remain red. It is acceptable to have red risks as long as the controls that manage the risk are periodically tested and found to be operating effectively.

### Tier Two Controls Assessment - Yellow Risks

Control assessment activities for Yellow Risks are very similar to those for Red Risks. The primary difference is that a Tier Two assessment does not require testing of controls. The following steps detail the activities associated with a Tier Two Controls Assessment.

#### 1. Identify Process Owners

The RM develops a list of individuals who have control over the policies, procedures, and controls related to the risk.

#### 2. Define Assessment Team

The RM establishes a team of personnel to conduct the assessment. Team members may include process owners, management analysts, contractors, or other resources available at the AU. These individuals should have knowledge of the processes related to the specific risk and should have experience with the assessment activities.

#### 3. Document Processes and Controls

The team identifies the related policies, procedures, and controls. When these are unavailable, the team will need to document policies, procedures and controls. This activity results in the development of process map documentation. The process maps provide details of activities, tasks, responsibilities, and key decision points in a given process. The purpose of process mapping is to identify control points in the process and the control activities performed by users.

#### 4. Conduct a Process Analysis

Once the documentation is available, the RM analyzes the information to help determine if there are adequate controls in place and if the controls are designed effectively. The analysis includes the identification of key controls to be tested.



### 5. Make a Management Decision

Based on the results of the process analysis, the RMO and RMs reach a decision about how to make improvements to the process that will mitigate the risk. Potential improvements to the process include:

- Creating new policies, procedures, or controls to address identified gaps.
- Modifying existing policies, procedures, or controls to address deficiencies.
- Redesigning the process to reduce risk exposure.
- Deciding to accept and monitor a risk if an unfavorable cost/benefit scenario is found.
- Developing some other solution to effectively mitigate the risk.

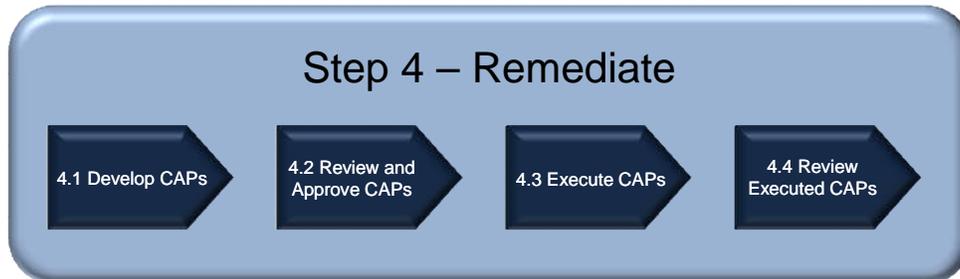
The management decision is incorporated into a Corrective Action Plan during the Remediate step of the Risk Management Methodology. This process is explained in the Remediate section of the Guidebook.

### Tier Three Controls Assessment - Green Risks

For Green risks, the RMO holds a meeting with the RMs and other key personnel knowledgeable about the risks. During this meeting, the risks are discussed in an open forum. While these risks do not require any immediate action, the purpose of the meeting is to raise the awareness of the risks throughout the organization. This awareness is critical in the event that the status of the risks change. Testing and documentation activities for Green risks are not required. However, if AUs have the time and resources available to conduct a Tier One or Tier Two control assessment of Green risks, they may do so.

### 4.0 Remediate

The results of the Assess step serve as the basis for determining the actions that must be taken during the Remediate step. This step consists of four major activities as shown below.



Documentation from the Remediate step supports the annual FMFIA statement of assurance along with documentation from steps two and three in the Risk Management Methodology. The activities that take place during this step demonstrate the organization's commitment to implementing and maintaining effective management processes, procedures, and controls.

#### 4.1 Develop Corrective Action Plans

At the beginning of the Remediate step, RMOs and RMs carefully consider the drivers behind the risk scores. They consider the factors that affect the impact and likelihood of each risk.

**Likelihood drivers** might include:

- The frequency of a transaction or a process.
- The complexity of the process.

**Impact drivers** might include:

- The scope of a risk.
- The lack of back-up systems.
- The lack of contingency plans.

After considering these drivers and the results of the Assess stage, RMOs and RMs determine remediation activities to address the risk. These are documented in a **Corrective Action Plan (CAP)**. *CAPs are detailed plans outlining the required activities to remediate a risk.* CAPs:

- Are based on the results of control assessments. The results of process analysis and tests of controls dictate what will be included in the CAP.
- Assign responsibility for remediation activities.



- Set appropriate deadlines for the completion of remediation activities.
- Outline the activities required to provide reasonable assurance that the impact or likelihood of a risk is reduced.

The RM leverages personnel who have direct knowledge of the process. These personnel are responsible for carrying out the corrective actions. A sample CAP template is shown below and may also be found in Appendix D.

### SAMPLE

National Institutes of Health		DRAFT				
Corrective Action Plan						
Assessable Unit	Risk Manager	Key Stakeholders				
Risk Description						
Date Identified (MM/DD/YY)						
Remediation Completion Date (MM/DD/YY)						
Action #	Action Description	Action Objective(s)	Action Owner(s)	Start Date	Due Date	Status
1						
2						
3						
4						
5						

Figure 17

Based on the results of the Assess step, the following actions may need to be documented in the CAP and executed by the RMs and other personnel.

- **Create a new policy, procedure, or control.** Management may have identified that a process is lacking the appropriate controls, which requires the creation of new controls.
- **Revise existing policies, procedures, or controls.** Management may determine that existing controls are out of date or ineffective. In this case, management determines which controls should be updated or revised in order to mitigate the risk.
- **Redesign the process.** If management identifies a risk that is associated with a particularly high risk process, they may decide that the process itself should be redesigned.

RMs assign responsibility to key personnel for completing corrective actions. RMs delegate this responsibility to personnel with the proper authority to implement the change. In some cases, the RM may need to complete the corrective actions themselves or reach out to the person in the organization with the proper authority.



### 4.2 Review and Approve Corrective Action Plans

The RMO reviews CAPs to help establish that the proposed actions will sufficiently mitigate the risk. The RMO verifies that specific individuals have been assigned responsibility for completing the actions in the CAPs according to reasonable and appropriate deadlines. The RMO works with the RM to improve the plan if necessary.

### 4.3 Execute Corrective Action Plans

Once the RMO approves the CAPs, RMs oversee and coordinate the execution of the specific actions that are outlined by the plan. RMOs are responsible for tracking the progress of remediation activities within the AU and ensuring that completion dates are being met. This requires the RMO to work closely with the RMs who directly oversee the execution of CAPs. Once remediation activities are complete and the changes have been in place for a minimum of three months, the controls assessment should be conducted again to determine whether the risk has been sufficiently mitigated through the implementation of the corrective actions.

### 4.4 Review Executed Corrective Action Plans

Once the actions have been completed in the CAPs, the RMO reviews the documents with the RM to verify sufficient completion. Executed CAPs are used to support the annual Statements of Assurance that must be signed by the Director of the AU. This documentation provides direct evidence of efforts that the AU has taken during the fiscal year to meet the requirements of OMB Circular A-123. Completed documentation is kept on record within the AU. In addition to these annual reporting requirements CAP progress should be reported quarterly to the RMO as part of the Report step.

### 5.0 Monitor

Continuous monitoring of risks is essential for the sustained success of the NIH Risk Management Program. Effective monitoring helps promote that controls continue to operate effectively. The Monitor step consists of one major activity as shown below.



The purpose of the Monitor step is to monitor risks for changes in status and take action on risks if they occur. In addition to this, AUs periodically re-score identified risks based on business rules established by OMA.

#### 5.1 Monitor the Risk Baseline

In order to work within the dynamic environment of NIH, risk monitoring should be done on a continuous basis. At any given time, it is likely that a new risk may occur, an existing risk may become obsolete or a risk's status may change in a variety of ways. Each RMO should define a process for their individual AU to continuously monitor risks. For this process, it may be helpful to reference the Organize the Process step of the Risk Management Methodology.

On a quarterly basis, the RMOC will meet to review the risk baseline, the status of each risk and related assessment and remediation efforts. In support of this meeting, OMA will issue a request to each AU to evaluate and make updates to their risk baseline information. Each AU's evaluation and update process should consider:

- Any new risks that may impact the organization and its ability to achieve the NIH mission. The AU should use the Risk Management Methodology to address each new risk.
- Whether any existing risks are no longer valid. The majority of the risk baseline will be comprised of inherent risks that will endure. Other risks may be specific to a program or project that is limited in its duration. Therefore, after the conclusion of such efforts, associated risks may be "retired."
- How the status of existing risks may have changed. If changes in the NIH or external environments have changed the potential impact or likelihood of the risk occurring, the AU should review the risk scoring questions and make changes as appropriate. Changes in a risk's score and position on the Risk Heat Map may change the necessary course of action to address the risk.



- Progress related to the risk assessment and remediation efforts. The AU should share progress that has been made against the controls assessment, remediation activities or other steps that relate to the tiered assessment approach.

Updates to information related to enterprise risks that are being managed across multiple AUs will require additional coordination for quarterly updates. The lead RMO for an enterprise risk should coordinate with the supporting AU RMOs to provide any necessary update information within the specified timeframe.

Information that is developed in the Monitor step will be utilized in the next step, Report.

### 6.0 Report

The Report step of the NIH Risk Management Methodology is critical in facilitating the communication of risk information. The Report step consists of one major activity as shown below.



### 6.1 Report

Following updates to the Risk Baseline made during the Monitor step, each AU will be required to report its new information. The formal mechanism for reporting, possibly an automated tool, has yet to be determined, but will be specified by OMA. The specific data elements required will also be specified by OMA.

Two types of formal reporting are currently planned.

**1. Quarterly Reporting.** As noted previously, risk information will be requested and reported to the RMOC on a quarterly basis. Information presented to the RMOC may be analyzed at the individual risk, Risk Category, AU or NIH-wide levels. Individual reports will be designed to share this information in a meaningful way that will support decision making about risks.

**2. Annual Reporting.** In addition to regular quarterly reports to the RMOC, each AU will also be required to provide an annual Statement of Assurance in support of FMFIA. Using a template provided by OMA, this Statement of Assurance should itemize the significant risks identified by each AU and the steps that have been or are being taken to assure the most effective and efficient use of federal resources. IC and OD office directors must sign a Statement of Assurance specific to their organization.



### Conclusion

This guidebook has provided an overview of how to conduct risk management activities at NIH. However, this document will require periodic updates and changes as the NIH Risk Management Program matures and evolves. As such, the guidebook must be considered a "living document" that will grow and change as the NIH Risk Management Program grows and changes. Recommendations and comments are welcome and may be submitted to OMA at [riskprogram@mail.nih.gov](mailto:riskprogram@mail.nih.gov).



### Appendix A - List of Acronyms

**AU** - Assessable Unit  
**CAP** - Corrective Action Plan  
**CC** - NIH Clinical Center  
**CCR** - Center for Cooperative Resolution  
**CIO** - Chief Information Officer, or Office of the Chief Information Officer  
**CIT** - Center for Information Technology  
**CSR** - Center for Scientific Review  
**ERO** - Enterprise Risk Owner  
**ES** - Executive Secretariat  
**FAM** - Federal Audit Manual  
**FIC** - John E. Fogarty International Center for Advanced Study in the Health Sciences  
**FMFIA** - The Federal Managers Financial Integrity Act (of 1982)  
**IC** - Institutes and Centers  
**IMOD** - Office of Extramural Research Immediate Office of the Director  
**JCAHO** - The Joint Commission on the Accreditation of Healthcare Organizations  
**NCCAM** - National Center for Complementary and Alternative Medicine  
**NCI** - National Cancer Institute  
**NCMHD** - National Center on Minority Health and Health Disparities  
**NCRR** - National Center for Research Resources  
**NEI** - National Eye Institute  
**NEO** - NIH Ethics Office  
**NHGRI** - National Human Genome Research Institute  
**NHLBI** - National Heart Lung and Blood Institute  
**NIA** - National Institute on Aging  
**NIAAA** - National Institute on Alcohol Abuse and Alcoholism  
**NIAID** - National Institute of Allergy and Infectious Disease  
**NIAMS** - National Institute of Arthritis and Musculoskeletal and Skin Diseases  
**NIBIB** - National Institute of Biomedical Imaging and Bioengineering  
**NICHD** - National Institute of Child Health and Human Development  
**NIDA** - National Institute on Drug Abuse  
**NIDCD** - National Institute on Deafness and Other Communication Disorders  
**NIDCR** - National Institute of Dental and Craniofacial Research  
**NIDDK** - National Institute of Diabetes and Digestive and Kidney Diseases  
**NIEHS** - National Institute of Environmental Health Sciences  
**NIGMS** - National Institute of General Medical Sciences  
**NIH** - National Institutes of Health  
**NIMH** - National Institute of Mental Health  
**NINDS** - National Institute of Neurological Disorders and Stroke  
**NINR** - National Institute of Nursing Research  
**NLM** - National Library of Medicine  
**OALM** - Office of Acquisition and Logistics Management  
**OAR** - Office of AIDS Research  
**OB** - Office of Budget  
**OBSSR** - Office of Behavioral and Social Sciences Research



**OCPL** - Office of Communications & Public Liaison  
**OD** - Office of the Director  
**ODEO** - Office of the Director Executive Office  
**ODP** - Office of Disease Prevention  
**OEODM** - Office of Equal Opportunity and Diversity Management  
**OER** - Office of Extramural Research  
**OFACP** - Office of Federal Advisory Committee Policy  
**OFM** - Office of Financial Management  
**OHR** - Office of Human Resources  
**OIR** - Office of Intramural Research  
**OLPA** - Office of Legislative Policy and Analysis  
**OM** - Office of Management  
**OMA** - Office of Management Assessment  
**OMB** - U.S. Office of Management and Budget  
**OPASI** - The Office of Portfolio Analysis and Strategic Initiatives  
**ORF** - Office of Research Facilities  
**ORS** - Office of Research Services  
**ORWH** - Office of Research on Women's Health  
**OSMP** - Office of Strategic Management Planning  
**OSP** - Office of Science Policy  
**RM** - Risk Manager  
**RMO** - Risk Management Officer  
**RMOC** - Risk Management Officer's Council  
**RO** - Risk Owner  
**SAT** - NIH Senior Assessment Team  
**WBS** - Work Breakdown Structure



### Appendix B - Glossary of Terms

#### **Assessable Unit (AU)**

Assessable Units (AUs) are discrete, mission-oriented sub-sets of an organization. At NIH, AUs reflect existing organizational structures to promote accountability. Each Institute and Center at NIH is an AU. Within the Office of the Director, there are 11 AUs based on strategic groupings of certain offices. For a detailed breakdown of AUs at NIH, refer to the graphic on page 8.

#### **Control**

Controls refer to the policies, procedures, or other processes that are designed to mitigate risks at an organization. Examples of controls at NIH include NIH Policy Manual Chapters, policies set at the HHS Department level, or requirements imposed on NIH by external third parties.

A control is:

- A mechanism to prevent or reduce the likelihood of a risk occurring.
- A means to reduce the impact of a risk should it occur.
- Designed to help promote the achievement of an organization's objectives, goals, and mission.
- Defined by organizational policies and procedures.
- A way to guide the daily activities of an organization and its employees.

#### **Control Gap**

A control gap requires the implementation of a control in an area that previously lacked an appropriate control. An example would be drafting a policy to address an area that previously lacked guidance or a formal process.

#### **Corrective Action Plan (CAP)**

CAPs are detailed plans outlining the required activities to remediate a risk. CAPs are based on the results of control assessment activities. The results of process analysis and tests of controls dictate what will be included in the CAP. They assign responsibility for remediation activities and set appropriate deadlines for the completion of remediation activities. CAPs also outline the activities required to provide reasonable assurance that the impact or likelihood of a risk is reduced.

#### **Design Deficiency**

A design deficiency exists when a control is not properly designed. For this type of deficiency, even if the control operates as designed, the control objective is not always met.

#### **Enterprise Risk Owner (ERO)**

The NIH Director is the Enterprise Risk Owner (ERO). Although the NIH Director is not responsible for carrying out the remediation of specific risks, he or she takes ownership of the full set of risks facing the organization based on his responsibility to sign the annual FMFIA statement of assurance.



### **Internal Control**

See the definition of "Control."

### **NIH Risk Management Methodology**

The NIH Risk Management Methodology is a customized six step approach that provides a standardized means of addressing risks at NIH.

### **NIH Risk Management Program**

The NIH Risk Management Program is an ongoing effort to perform standardized repeatable activities that promote the overall efficiency, effectiveness, accountability and integrity of the organization's work. This program is endorsed by the NIH Steering Committee, and is designed to proactively identify and manage risks before they become obstacles to the NIH mission.

### **Operating Deficiency**

An operating deficiency exists when a properly designed control does not operate as intended, or when the person performing the control does not possess the necessary authority or qualification to perform the control effectively.

### **Risk**

A risk is an uncertain event or condition that may have a negative impact on an organization. A risk is any event or condition that threatens the achievement of the objectives, goals, or mission of an organization. A risk is uncertain because it pertains to something that may occur in the future.

### **Risk Baseline**

The Risk Baseline is an enterprise-wide portfolio of risks that serves as a reference point for further risk management activities.

### **Risk Capture Form**

The Risk Capture Form is a standardized data entry tool for capturing risk information. It brings consistency to the process of identifying and scoring risks across a large and disparate agency. Detailed information regarding the Risk Capture Form is found in Appendix C.



### **Risk Category**

A Risk Category is a mechanism by which risks are logically grouped with other related risks. The categories are aligned to major OD and IC functional areas to provide enhanced reporting capabilities to the Risk Management Program. Risk Categories include:

<b>Acquisitions</b>	<b>Information Management</b>
<b>Financial</b>	<b>Intramural</b>
<b>Human Capital</b>	<b>Extramural</b>
<b>Facilities</b>	<b>Other</b>

Additional information regarding risk categories can be found in Appendix C.

### **Risk Heat Map**

A Risk Heat Map is a graphical representation of identified risks. It is a tool used to illustrate the magnitude of a risk measured in terms of Impact and Likelihood. Additional information can be found on page 26.

### **Risk Impact**

Risk Impact is the potential effect that a risk may have. At NIH, Risk Impact is quantified by assigning a numerical score based on responses to questions on the Risk Capture Form. Risk Impact is one of the two dimensions that contribute to the overall Risk Score (the other dimension is Risk Likelihood).

### **Risk Likelihood**

Risk Likelihood represents the chance that a risk may occur. At NIH, Likelihood is quantified by assigning a numerical score to standardized questions on the Risk Capture Form. Risk Likelihood is one of the two dimensions that contribute to overall Risk Score (the other dimension is Risk Impact).

### **Risk Manager (RM)**

Risk Managers (RMs) are responsible for identifying and scoring risks using the Risk Capture Form. Once risks have been assessed according to the tiered approach, RMs work with the RMO to remediate risks. Additional information regarding this role can be found on page 12.

### **Risk Management**

Risk management is a continuous process, carried out by the members of an organization, designed to proactively identify and mitigate risks to help promote the achievement of the organization's objectives, strategy, and mission.

### **Risk Management Organizational Framework**

The NIH Risk Management Organizational Framework is an arrangement of the agency to facilitate risk management activities at the enterprise level.



### **Risk Management Guidebook**

The Risk Management Guidebook is a detailed reference for carrying out risk management activities at NIH. It includes an introduction to risk management principles and explains the value of risk management. The Guidebook provides a detailed explanation of each step in the NIH Risk Management Methodology, including guidance on how to perform each step.

### **Risk Management Officer (RMO)**

A Risk Management Officer is an individual who is designated to oversee the Risk Management activities within an Assessable Unit. The RMO works closely with the Risk Owner and Risk Managers in each step of the NIH Risk Management Methodology. Additional information regarding this role can be found on page 11.

### **Risk Management Council (RMC)**

The RMC is a grouping of NIH senior leaders, established to advise, support and provide a resource to the NIH Steering Committee on policies and procedures related to the NIH Risk Management Program.

### **Risk Management Structure**

A risk management structure is a segmentation of an AU to facilitate risk management activities at the AU level. A risk management structure allows the divisions, offices, and functions within an AU to be involved in the risk management process. The structure also allows organizations to clearly assign ownership of risks to the appropriate personnel.

### **Risk Owner (RO)**

A Risk Owner is the individual who has the authority to manage risks and/or controls within an Assessable Unit. The RO is typically the director of the AU, and each RO is ultimately responsible for the risks that exist within their AU. The RO is responsible for signing the annual statement of assurance for the IC or OD Office. Additional information regarding this role can be found on page 10.

### **Risk Score**

The Risk Score is the sum of the points assigned to an individual risk based on the responses to the Impact and Likelihood questions on the Risk Capture Form. Risk Scores allow for quantitative comparison and ranking of risks across NIH.

### **Risk Statement**

A risk statement is a detailed description of a potential risk and its perceived effect. Additional information regarding risk statements can be found on page 19.

### **Risk Validation**

Risk validation is a process in which risk data is reviewed, discussed, and clarified in order to gain a thorough understanding of the risk before it is finalized.



### **Steering Committee**

The NIH Steering Committee is an organization that serves to support and provide guidance to the NIH Director. With regard to risk management, the Steering Committee:

- Exercises stewardship over the use of NIH resources and provides oversight to promote programs that operate within established standards.
- Provides policy guidance and general oversight to support the successful completion of the yearly FMFIA statements of assurance.
- Provides recommendations to the NIH Director on required changes in policies, procedures, and resources to promote the successful operation of the NIH Risk Management Program.
- Provides a high-level summary of activities occurring within the Risk Management Council (RMC).

### **Tiered Risk Assessment Approach**

The tiered risk assessment approach is a method for determining the requirements for assessing risks based on their severity. Additional information is found on page 28.



### Appendix C - The Risk Capture Form

The Risk Capture Form is a standardized data entry tool for capturing risk information. It brings consistency to the process of identifying and scoring risks across a large and disparate agency. The NIH Risk Capture Form consists of four major sections. Each of these sections and the data fields within them are described below.

#### User Information:

##### (1) Name

The user enters his/her first and last name.

##### (2) Date

The user enters the date that the risk was identified.

##### (3) Position/Title

The user enters his/her position or title within the organization.

##### (4) Assessable Unit

The user enters the AU of which he/she is a part.

##### (5) Division/Office

The user enters the division or office in which they work. This should correspond to the risk management structure defined by the AU.

##### (6) Email Address

The user enters his/her NIH email address.

##### (7) Telephone Number

The user enters his/her NIH telephone number.

#### Risk Identification:

##### (8) Risk Statement

A risk statement is developed using an "if-then" format. By focusing on phrasing risk statements this way, a standardized approach is brought to the process, and risk statements are created in a similar fashion. The "if" portion of the risk statement should relate to an uncertain event or condition that may occur. The "then" portion of the risk statement should describe the potential outcome of the risk. See page 19 for guidance.

##### (9) Immediacy

Risk Immediacy relates to the timeframe in which the risk may occur. For certain risks, it may not be possible to estimate a timeframe for occurrence. If the risk is no more likely to occur at



one time than another, select "N/A" from the menu. For other risks, such as those related to the completion of a certain project or protocol, it may be possible to determine when the risk would occur. In this case, use your judgment to select the appropriate timeframe from the menu.

### (10) Span of Control

Span of Control indicates whether or not the risk can be directly managed by NIH. In other words, Span of Control attempts to determine if someone at NIH can take an action to reduce the risk. If the risk cannot be controlled by NIH, then it is considered an external risk.

### (11) Risk Category

A Risk Category is a mechanism by which risks are logically grouped with other related risks. NIH risk categories are aligned to major functional areas to provide enhanced reporting capabilities to the Risk Management Program. Risk Categories are selected on the Risk Capture Form to provide information about the functional groupings that apply to the risk. Up to three categories can be selected for any given risk. Risk Categories enhance the reporting capabilities of the Risk Management Program, making it possible to analyze the data and gain an understanding of which functional areas have the greatest risk. Risk categories used at NIH include the following:

<b>Acquisitions</b> <i>This category includes risks related to acquisitions and logistic activities related to contracts.</i>	<b>Financial</b> <i>This category includes financial related risks such as budget, travel and intellectual property activities at NIH.</i>	<b>Human Capital</b> <i>This category includes human resource related issues including recruitment, retention &amp; personnel management.</i>	<b>Facilities</b> <i>This category includes risks related to building, managing, &amp; maintaining facilities, property &amp; equipment.</i>
<b>Information Management</b> <i>This category includes risks related to IT, IT security, and records management.</i>	<b>Intramural</b> <i>This category includes risks related to intramural research activities.</i>	<b>Extramural</b> <i>This category includes risks related to extramural research activities.</i>	<b>Other</b> <i>This category includes other risks not included in the designated categories.</i>

The following are examples of potential risks listed by category. This is not an all-inclusive list, rather this list is intended to stimulate ideas and serve as a tool to assist personnel in the task of risk identification. Based on an individual's responsibilities they may identify risks in all categories, or only a select few. For risks that do not readily apply to an established category, there is an "other" category.



### Acquisitions

Examples of potential *Acquisitions Risks* Include:

- If NIH relies on a limited number of suppliers, then personnel may be unable to obtain critical materials or services in times of shortage or urgent need.
- If NIH fails to pay vendors and contractors in a timely manner, then they may become unwilling to do business with NIH.
- If NIH fails to be proactive in identifying quality issues from certain vendors, then NIH may continue to obtain inferior goods and services from these vendors.

### Financial

Examples of potential *Financial Risks* Include:

- If the use of NIH purchase cards is not appropriately tracked, then waste, fraud and abuse of government funds may occur.
- If NIH does not properly track improper payments, then violations of the Improper Payments Information Act (IPIA) may occur, and there may be waste, fraud, and abuse of government funds.
- If NIH fails to effectively track sponsored travel arrangements for researchers and scientists, then waste, fraud, and abuse of government funds may occur.

### Human Capital

Examples of potential *Human Capital Risks* Include:

- If NIH is unable to attract scientific personnel to conduct research, then the agency's ability to achieve its scientific mission will be threatened.
- If NIH employees and staff do not have adequate opportunities for career development and advancement, then excessive turnover may occur.

### Facilities

Examples of potential *Facilities Risks* Include:

- If the NIH Clinical Center fails to meet accreditation requirements, then the operation of the Clinical Center may be jeopardized.
- If NIH is unable to track asbestos abatement activities, then employee and patient health may be threatened.
- If NIH facilities are shut down due to broken water pipes, loss of electricity, loss of climate control, etc., then scientific personnel cannot carry out the scientific mission and significant costs may be incurred to correct the problem(s).

### Information Management

Examples of potential *Information Management Risks* Include:

- If information technologies used at NIH are not operating as intended, then this could potentially result in the exposure of data and financial assets to loss or misuse.



- If unsecure systems and databases exist, then data corruption, misuse or dissemination of sensitive information due to a network attack or penetration may occur.
- If an unencrypted laptop is stolen, then a significant degradation of public trust may occur and patient data is compromised.

### Intramural

Examples of potential *Intramural Risks* Include:

- If there is an occurrence of a major environmental health and safety incident, then the NIH campus may shutdown.
- If improper treatment of animals used for scientific research activities occurs, then NIH will receive negative publicity that impacts the public's trust in NIH.
- If human subject volunteers suffer unnecessary health consequences due to participation in a clinical trial, then NIH may receive negative publicity and a decline in public trust.

### Extramural

Examples of potential *Extramural Risks* Include:

- If there are flaws in the grant application and peer review process, then there may be a decline of principal investigators (PIs) applying or re-applying for research grants.
- If there is a lack of NIH supervision over grantee research activities, then this could result in the misuse of government funds by grantees and a decline in public trust.

### Other

Examples of potential *Other Risks* Include:

- If there is a natural disaster (Fire, Flood, Tornado, Earthquake, etc.) or other disasters stopping or slowing NIH operations, then NIH cannot achieve its mission goals.
- If there is a decrease in the number of principal investigators seeking NIH grants, then the scientific research efforts at NIH are diminished.

## **(12) What are the primary policies, procedures, and controls in place to manage this risk?**

Policies, Procedures, and Controls are the mechanisms in place to manage the risk. Collectively, NIH policies and procedures are broadly referred to as "controls." Examples of controls include NIH Policy Manual Chapters or any other documented process that relates to the risk. These controls may often exist within a specific IC or OD Office, rather than being an NIH-wide control. This element on the Risk Capture Form is used to identify known policies, procedures, and controls that apply to the identified risk. If no controls exist, it should be noted in this field.



### **(13) What Metrics are in place to track this risk?**

Metrics are performance measures used by management to determine the performance of a certain function or process. For example, if a certain policy at NIH requires scientific directors to review and sign a document, the related metric would calculate the percentage of documents that have been reviewed and signed out of the population. Risk identifiers are encouraged to identify applicable metrics that can be used to gauge the performance of a function or process as it relates to the identified risk.

### **(14) Please use the space below to provide any comments or additional information regarding this risk.**

Additional Comments can be provided on any topic that is not covered on the Risk Capture Form. The quality of risk data is enhanced when more information is provided.

#### **Risk Impact:**

For each of the Risk Impact questions asked, select just one answer. Use your best judgment and try to maintain an "Enterprise" perspective while answering.

### **(15) What is the Impact on the NIH mission?**

Responses to this question include:

- a) The risk could have a minimal effect on the NIH mission.
- b) The risk could have a significant effect on the NIH mission.
- c) The risk could have a severe effect on the NIH mission.

### **(16) What is the Impact on public trust?**

Responses to this question include:

- a) The risk could have a minimal effect on the public trust.
- b) The risk could have a significant effect on the public trust.
- c) The risk could have a severe effect on the public trust.

### **(17) What is the Organizational Impact?**

Responses to this question include:

- a) The risk could affect a single office, department, or division.
- b) The risk could affect more than one OD Office or IC.
- c) The risk could affect all of NIH or extends beyond NIH.

### **(18) What is the Financial Impact?**

Responses to this question include:



- a) The risk could result in a financial impact of up to \$500,000.
- b) The risk could result in a financial impact ranging between \$500,000 and \$5 million.
- c) The risk could result in a financial impact greater than \$5 million.

### **(19) Professional Judgment**

Responses to this dimension include:

- a) In my professional judgment, the risk could have a minimal overall impact on the NIH.
- b) In my professional judgment, the risk could have a significant overall impact on the NIH.
- c) In my professional judgment, the risk could have a severe overall impact on the NIH.

### **Risk Likelihood:**

For each of the Risk Likelihood questions asked, select just one answer. Use your best judgment and try to maintain an "Enterprise" perspective while answering.

### **(20) Are written policies, procedures, or controls in place to manage this risk?**

Examples of policies, procedures, and controls include NIH Policy Manual chapters, or any other documented processes that are followed related to this risk.

Responses to this question include:

- a) Yes.
- b) No.

### **(21) Written policies, procedures, or controls are effective (if applicable).**

If policies, procedures, or controls exist, indicate how well they are followed in the organization. Do the policies, procedures, and controls have a strong influence over daily operations? If so, then they are likely to be effective. If policies, procedures, and controls are not closely followed, they are likely ineffective.

Responses to this statement include:

- a) Strongly Agree.
- b) Agree.
- c) Disagree.
- d) Strongly Disagree.

### **(22) Are all policies included as Manual Chapters in the NIH policy manual?**



If policies are not included in the NIH policy manual, then answer "no" to this question. Only answer "yes" if policies exist as manual chapters. (NIH requires that all NIH policy manual chapters be updated every five years).

Responses to this question include:

- a) Yes - Policy manual chapters exist.
- b) No - Policy manual chapters do not exist.

### **(23) Individuals within my organization (Assessable Unit) are aware of this risk.**

This question addresses the overall level of awareness of the risk in the organization. Is awareness of this risk limited to a small group of people? Or is there widespread awareness of this risk throughout the organization?

Responses to this statement include:

- a) Strongly Agree.
- b) Agree.
- c) Disagree.
- d) Strongly Disagree.

### **(24) Is management taking formal actions to mitigate or address this risk?**

Is management sponsoring a training and education program, redesigning the process, conducting a management review, issuing authoritative guidance, etc.?

Responses to this question include:

- a) Yes.
- b) No.

### **(25) In your professional judgment, what is the likelihood that the identified risk could occur?**

Using your best judgment, select the response that most closely represents the chance of the risk occurring.

Responses to this question include:

- a) Very Unlikely.
- b) Unlikely.
- c) Likely.
- d) Very Likely.



# NIH Risk Management Guidebook

## Appendix C - The Risk Capture Form

National Institutes of Health Risk Capture Form	
User Information	<p><b>Instructions</b> Please complete all fields in the Risk Capture Form for each risk that you identify.</p> <p>1. Name <input type="text"/>      2. Date (mm/dd/yyyy) <input type="text"/>      3. Position/Title <input type="text"/></p> <p>4. Assessable Unit (Click on box to select from drop-down menu) <input type="text"/>      5. Division/Office <input type="text"/></p> <p>6. Email Address <input type="text"/>      7. Telephone Number <input type="text"/></p>
	<p>8. Risk Statement Use the two fields below to write an "if-then" statement for the risk you are identifying.</p> <p>If... <input type="text"/></p> <p>then... <input type="text"/></p> <p>9. Immediacy (click on box to select from the drop-down menu) <input type="text"/>      11. Risk Category Select up to three risk categories below.</p> <p>10. Span of Control (click on box to select from drop-down menu) <input type="text"/>      <input type="text"/></p> <p>12. What are the primary policies, procedures, and controls in place to manage this risk? (type your response below)</p> <p><input type="text"/></p> <p>13. What metrics are in place to track this risk? (type your response below)</p> <p><input type="text"/></p> <p>14. Please use the space below to provide any comments or additional information regarding this risk.</p> <p><input type="text"/></p>
Risk Impact	<p>15. What is the Impact on the NIH Mission? (click on box to select from drop-down menu) <input type="text"/></p> <p>16. What is the Impact on Public Trust? (click on box to select from drop-down menu) <input type="text"/></p> <p>17. What is the Organizational Impact? (click on box to select from drop-down menu) <input type="text"/></p> <p>18. What is the Financial Impact? (click on box to select from drop-down menu) <input type="text"/></p> <p>19. Professional Judgment. (click on box to select from drop-down menu) <input type="text"/></p>
Risk Likelihood	<p>20. Are written policies, procedures, or controls in place to manage this risk? GUIDANCE: Examples of policies, procedures, and controls include NIH Policy Manual chapters, or any other documented processes that are followed related to this risk.</p> <p><input type="checkbox"/> NOTE: If you answer "No," please skip questions 14 and 15 as they do not apply (you can leave them blank).</p> <p>21. Written policies, procedures, or controls are effective (if applicable). GUIDANCE: The following questions may indicate the effectiveness of controls: If policies, procedures, or controls exist, how well are they followed in the organization? Do personnel have a negative attitude towards them? Or is there a culture of compliance that seeks to closely adhere to authoritative guidance on the issue?</p> <p><input type="text"/></p> <p>22. Are all policies included as Manual Chapters in the NIH policy manual?</p> <p><input type="text"/></p> <p>23. Individuals within my organization (Assessable Unit) are aware of this risk. GUIDANCE: Are you the only person who knows about this risk? Or is there widespread awareness of this risk throughout your organization?</p> <p><input type="text"/></p> <p>24. Is management taking formal actions to mitigate or address this risk? GUIDANCE: Is management sponsoring a training and education program, redesigning the process, conducting a management review, issuing authoritative guidance, etc.?</p> <p><input type="text"/></p> <p>25. In your professional judgment, what is the likelihood that the identified risk could occur?</p> <p><input type="text"/></p>



# NIH Risk Management Guidebook

## Appendix D - Corrective Action Plan (CAP) Template

### Appendix D - Corrective Action Plan (CAP) Template

The following represents a sample CAP that could be used to support the Remediate step of the NIH Risk Management Methodology.

**SAMPLE**

National Institutes of Health		DRAFT				
Corrective Action Plan						
Assessable Unit	Risk Manager	Key Stakeholders				
Risk Description						
Date Identified (MM/DD/YY)	Remediation Completion Date (MM/DD/YY)					
Action #	Action Description	Action Objective(s)	Action Owner(s)	Start Date	Due Date	Status
1						
2						
3						
4						
5						



### Appendix E - Frequently Asked Questions

#### Question: How does NIH define risk?

**Answer:** Risks are uncertain events or conditions that could negatively impact NIH. Risks come in many forms, and some risks are much more critical than others depending on their potential Impact and Likelihood of occurrence.

#### Question: How can I begin to identify risks?

**Answer:** Risks can be identified by thinking about the potential events or conditions that could threaten the achievement of the goals and objectives of a project, program, or the organization as a whole. The Risk Capture Form has been developed to document the risks that you identify.

#### Question: Is it my job to identify every risk that affects my area of responsibility?

**Answer:** You are not expected to identify every potential event or condition that could have a negative impact on your area of responsibility. It is not feasible to identify and manage the full universe of risks that exist at NIH.

#### Question: How can I determine which risks are the most critical?

**Answer:** If an event or condition might prevent the achievement of the goals and objectives of a single project or program, it would be considered less critical than a risk that threatens the achievement of the NIH scientific mission. Think about those events or conditions that would result in the most significant negative result on the organization, a program, or a project.

#### Question: How often do I need to identify risks?

**Answer:** Identifying risks is done on an annual basis at NIH. However, risk identification can be a continuous process by following the guidelines provided below.

- ✓ You should get in the habit of considering risk in every project, program, supporting service, or line of research that you are involved with.
- ✓ Risks should be documented on a continual basis as they come to your attention.
- ✓ If a previously identified risk changes in terms of its Impact and Likelihood (i.e., becomes more or less critical), you should document this change.

#### Question: What kind of support can I expect?

**Answer:** OMA will be providing support to OD offices and ICs throughout the process. This support will include the provision of various tools, templates, training, and guidance designed to assist those performing risk management activities.



**Question: Risk management was done differently at my old organization. Why?**

**Answer:** The NIH Risk Management Program was developed based on the specific and unique needs of NIH. While it includes many aspects of other risk management programs, some elements have been tailored to fit the culture, environment, and mission of NIH as well as the goals of its Sr. Management.



### Appendix F - Reference

This appendix provides a list of key references that relate to the NIH Risk Management Program.

#### **The OMA Risk Management Website**

<http://oma.od.nih.gov/ma/NewRisk/>

The Office of Management Assessment (OMA) is responsible for developing and maintaining the NIH Risk Management Program. The OMA risk management website provides information and updates on the Program.

#### **The Federal Manager's Financial Integrity Act (FMFIA)**

<http://www.whitehouse.gov/omb/financial/fmfia1982.html>

FMFIA legislation requires government agencies to implement effective controls to provide reasonable assurance that:

- (i) Obligations and costs are in compliance with applicable law.
- (ii) Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation.
- (iii) Revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

#### **The Office of Management and Budget: Circular A-123**

[http://www.whitehouse.gov/omb/circulars/a123/a123\\_rev.pdf](http://www.whitehouse.gov/omb/circulars/a123/a123_rev.pdf)

The Office of Management and Budget (OMB) issues Circular A-123, "Management's Responsibility for Internal Control." This document provides guidance on meeting the requirements of the Federal Manager's Financial Integrity Act (FMFIA) of 1982.

#### **COSO Enterprise Risk Management Framework: Executive Summary**

[http://www.coso.org/Publications/ERM/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) Framework applies primarily to publicly traded companies. However, its core principles serve as a conceptual foundation for the NIH Risk Management Program.