NIH Policy Manual

1750 - NIH Risk Management Program

Issuing Office: OD/OM/OMA **Phone:** (301) 496-1873

Release Date: 8/04/2017 ?

Transmittal Notice

1. **Explanation of Material Transmitted:** This chapter outlines responsibilities for complying with the National Institutes of Health (NIH) Risk Management Program. This revision incorporates changes required by the Office of Management and Budget's 2016 updates to its Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (OMB Circular A-123) pertaining to Enterprise Risk Management.

   Please refer to Integrity Act Statement of Assurance and Reporting for NIH's responsibilities pertaining to the agency's annual Statement of Assurance and the Federal Managers' Financial Integrity Act of 1982 reporting processes.

2. **Filing Instructions:**

   Remove: NIH Manual Chapter 1750, dated 08/14/14
   Insert: NIH Manual Chapter 1750, dated 08/04/17

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Policy Manual, contact the Division of Management Support, OMA on 301-496-4606, or enter this URL: https://oma.od.nih.gov/DMS/Pages/Manual-Chapters.aspx.

A. Purpose

This manual chapter outlines responsibilities for complying with the NIH Risk Management Program (RM Program). NIH designed the RM Program to help identify and manage risks, processes, and controls that may affect NIH's ability to achieve its mission, strategic goals, and objectives. The RM Program provides a framework for improving programs and operations within the agency's extramural, intramural, and administrative components.

B. Scope

This policy applies to all NIH Institutes and Centers (IC), Office of the Director (OD) offices, and all NIH staff.

C. Authority

This policy is issued under the authority of the Federal Managers' Financial Integrity Act (FMFIA) of 1982 and OMB's Circular A-123.

D. References

1. NIH Risk Management web site at https://oma.nih.gov/RMAL/NIHRM/default/default.aspx (NIH access only)
2. NIH Enterprise Risk Management Guidebook for ICs and OD Offices at https://oma.nih.gov/RMAL/NIHRM/default/Risk%20Management%20Guidebook/Introduction.aspx (NIH access only)
3. NIH Manual Chapter 1755 Integrity Act Statement of Assurance and Reporting at https://policymanual.nih.gov/1755
4. Federal Manager's Financial Integrity Act of 1982 at https://www.dol.gov/ocfo/media/regs/FMFIA.pdf
5. OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (revised), July 15, 2016, at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf
6. OMB Circular A-11, Preparation, Submission, and Execution of the Budget (revised), Section 270.24, July 1, 2016, at https://obamawhitehouse.archives.gov/omb/circulars_a11_current_year_a11_toc
7. Government Performance and Results Act of 1993 at https://www.dol.gov/ocfo/media/regs/GPRA.pdf and Government Performance and Results Modernization Act of 2010 at https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf
8. GAO Standards for Internal Control in the Federal Government, dated September 2014 at http://www.gao.gov/assets/670/665712.pdf
9. NIH Manual Chapter 1743,"Keeping and Destroying Records," Appendix 1, NIH Records Control Schedule at https://policymanual.nih.gov/1743

E. Background

Risk management is a continuous process performed by staff at all levels of an organization, designed to proactively identify and manage risks to help promote the achievement of program and project objectives. Risk management activities involve identifying, assessing, managing, monitoring, and reporting on risks and associated controls. These activities form a continuous cycle that is embedded in all of the organization's practices and business

processes.

Enterprise Risk Management (ERM) is a strategic discipline that seeks to deliberately and proactively understand the full spectrum of risks including opportunities across all organizational silos, and integrates them into an enterprise-wide, strategically aligned, and interrelated risk portfolio view.

Risk management and ERM practices improve the efficiency and effectiveness of government operations. They are designed to enhance management decision-making, alleviate potential risks, be forward-looking, and identify previously unknown opportunities.

F. Policy

The RM Program divides NIH into 38 units for purposes of identifying and reporting on risks. This policy refers to the units collectively as IC/OD Office(s). A list of designated units (NIH access only) is available on the NIH RM Program web site under the Organizational Framework tab.

Federal leaders and managers are responsible for establishing goals and objectives, ensuring compliance with relevant laws and regulations, and managing both expected and unanticipated risk events. They are responsible for implementing management practices that identify, assess, manage, monitor, and report on risks. Risk management practices must be taken into account when designing internal controls and assessing their effectiveness. The NIH Director, NIH Principal Deputy Director, NIH Deputy Director for Management, IC/OD Office Directors, Risk Management Officers, Risk Management Champions, and Risk Managers are required to carry out specific responsibilities for implementing and maintaining risk management programs, and reinforcing a culture of risk management and accountability, as set out in Section G of this policy.

Effective ERM cannot be performed in isolation, therefore NIH employs a holistic approach whereby it integrates risk management and ERM practices into NIH's daily operations, as well as strategic planning, budgeting, and performance management across all programs and activities. The NIH Enterprise Risk Management Guidebook for ICs and OD Offices supports this policy by describing the NIH RM Program Methodology and processes associated with each required activity outlined below.

1. Execute all phases of NIH's Risk Management Methodology:

    a. Phase #1 – Strategic Goals:

        i. IC/OD Offices will review available mission-related strategic plan(s) and understand the associated goals and objectives, and
        ii. IC/OD Offices will consider the parameters of operating constraints when planning their risk management activities.

    b. Phase #2 - Identify and Score:

i. IC/OD Offices will identify and score risks that have the potential to impact the achievement of the IC/OD Office's mission, strategic goals, and objectives, and
ii. IC/OD Offices will enter risks into the NIH central risk management data repository and will designate enterprise risks according to the requirements set forth in the NIH Enterprise Risk Management Guidebook for ICs and OD Offices.

c. Phase #3 - Assess:

i. IC/OD Offices will participate in and support assessments conducted by the Office of Management Assessment (OMA), as set forth in Section I of this policy,
ii. IC/OD Offices will conduct internal IC/OD Office assessments to adequately manage their risks, and
iii. IC/OD Offices will notify OMA immediately upon a determination of a potential material weakness as defined within OMB Circular A-123. OMA will then notify the NIH Chief Financial Officer of the potential material weakness because of their responsibilities pertaining to the agency's annual Statement of Assurance.

d. Phase #4 – Manage:

i. IC/OD Offices will develop and document appropriate risk responses including action plans, as needed, for their enterprise risks according to the requirements and standards of quality set forth in Appendix A of the NIH Enterprise Risk Management Guidebook for ICs and OD Offices.

e. Phase #5 – Monitor:

i. IC/OD Offices will routinely monitor their risk environment, identify and score new risks, review existing risks for continued applicability, and rescore risks based on current circumstances,
ii. IC/OD Offices will monitor the status of risk responses, and
iii. IC/OD Offices will monitor the effectiveness of internal controls as a normal course of business. Reviews, reconciliations or comparisons of data should be included as part of the regularly assigned duties of personnel. In addition, IC/OD Offices should integrate periodic internal IC/OD Office assessments as part of management's continuous monitoring of internal controls.

f. Phase #6 – Report:

i. IC/OD Offices will provide OMA with an annual risk inventory update that summarizes the reassessment of their risk inventories in the NIH central risk management data repository,

ii. Individuals or IC/OD Offices designated as owners of NIH ERM risks will provide OMA with periodic status updates when requested, and
iii. IC/OD Offices will provide OMA with a supporting annual FMFIA Statement of Assurance, as set out in Section H of this policy.

2. NIH and IC/OD Offices will use ERM and risk management data and other relevant information as an integral part of the decision-making process at all levels within the organization, and maintain documentation that supports the rationale for management decisions involving risks that have the potential to significantly impact the achievement of mission, strategic goals, and objectives.
3. IC/OD Offices will ensure that employees who are assigned risk management program roles understand their responsibilities and can execute RM Program requirements.

G. Roles and Responsibilities

1. **NIH Director and Principal Deputy Director** – Provide executive sponsorship for RM Program, determine NIH strategic goals and objectives, designate NIH ERM risks and oversee progress on NIH ERM risk management activities.
2. **IC/OD Office Directors** – Establish a culture of risk management excellence and integrity within the IC/ OD Office, determine IC/OD strategic goals and objectives, designate IC/OD Office ERM risks and oversee progress on IC/OD ERM risk management activities.
3. **Risk Management Officers** – Plan, coordinate, and manage the IC/OD Office risk management programs, assess and report on IC/OD Office internal controls, and facilitate determination and prioritization of IC/OD ERM risks.
4. **Risk Management Champions** – Serve as a liaison between Risk Management Officer, Risk Managers, and the Office of Management Assessment and provide risk management support to their Risk Management Officer.
5. **Risk Managers** – Ensure compliance with applicable laws, regulations, and policies. Identification, management and accountable acceptance of risk, within his/her functional area. This includes the identification and management of potential fraud risks.
6. **NIH Employees** – Embrace the NIH risk management culture that promotes open and candid risk identification and management, and execute controls in compliance with laws, regulations, policies, and procedures.
7. **Deputy Director for Management** – Serve as the NIH Chief Financial Officer and is responsible for managing the RM Program.
8. **Office of Management Assessment** – Develop and maintain the NIH RM Program policy and guidance, provide risk management expertise and guidance to IC/OD Offices, and conduct assessments and reviews, as set out in Section I.

H. Federal Manager's Financial Integrity Act

The Federal Manager's Financial Integrity Act (FMFIA) and OMB Circular A-123 require every Department-level agency to provide assurances on internal control effectiveness in its Agency Financial Report or the Performance and Accountability Report. NIH submits summary information to the Department of Health and Human Services about the effectiveness of NIH's internal controls.

The objectives of FMFIA are to ensure:

1. effective and efficient operations,
2. compliance with applicable laws and regulations, and
3. reliable financial reporting.

OMB Circular A-123 requires NIH to continually monitor, assess, and improve the effectiveness of internal controls. As such, IC/OD Offices must provide annual assurance to the NIH Director on the state of their internal controls.

IC/OD Offices will:

1. provide OMA with an annual Statement of Assurance signed by the IC/OD Office Director and enter supporting data for the current fiscal year into the NIH central risk management data repository,
2. maintain documentation supporting their annual Statement of Assurance,
3. conduct internal control reviews within their organization to ensure internal controls are operating effectively and efficiently, and
4. provide information and documentation to support the Office of Financial Management efforts to review internal controls over financial reporting.

I. Risk and Control Assessments and Special Management Reviews

At the request of NIH senior leadership, OMA periodically performs assessments or reviews that may span across multiple NIH organizations. When requested, OMA will:

1. perform a risk assessment, control assessment, or management review in accordance with NIH senior leadership's approved list of targeted areas,
2. develop a draft report outlining findings and recommendations,
3. distribute the draft report to the subject(s) of the review for comment, and
4. disseminate a final report and recommendations to the appropriate parties including the NIH Director and Principal Deputy Director.

J. Definitions

Accountable Acceptance of Risk: Accountable acceptance of risk is the Risk Manager consciously accepting some level of risk in order to effectively allocate resources because of competing priorities in alignment with strategic goals and objectives.

Enterprise Risks: Enterprise risks are risks prioritized by senior leadership as having the greatest potential to affect the organization's ability to achieve its mission. Enterprise risks have a direct correlation to the organization's strategic goals and objectives supporting the mission. Senior leadership is actively engaged in overseeing or managing enterprise risks.

Internal Control: An internal control is a mechanism to detect, prevent or reduce the likelihood of a risk occurring, or an activity to correct or lessen the impact of a risk should an event occur.

Interrelated Risk Portfolio: An interrelated risk portfolio provides insight into areas of risk exposure across multiple organizational silos, thus increasing an organization's chances of executing a better assessment of risk, experiencing fewer unanticipated outcomes, and improving the quality of decision-making.

Material Weakness: A material weakness may impair NIH's fulfillment of essential operations or mission. It may also be significant enough to impact management's internal or external decision-making. A material weakness may significantly weaken established safeguards against fraud, waste, loss, unauthorized use, or misappropriation of funds, property, other assets, or conflicts of interest. A material weakness in internal control over compliance is a condition where management lacks a process that reasonably ensures preventing a violation of law or regulation that has a direct and material effect on financial reporting or significant effect on other reporting or achieving NIH objectives.

Risk: A risk is the possibility that an event or condition, both positive (opportunity) and negative (challenge) may occur that would impact an organization. All activities at every level of an organization involve some risk.

Additional definitions and supporting guidance are located in the NIH Enterprise Risk Management Guidebook for ICs and OD Offices (Section D: References, #2).