NIH Policy Manual

1750 - NIH Risk Management Program

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

Release Date: 10/23/2023 ?

Transmittal Notice

1. **Explanation of Material Transmitted:** This chapter outlines the functional responsibilities for the National Institutes of Health (NIH) Institutes, Centers, and Offices (ICOs) for complying with the NIH Risk Management Program (RM Program). This revision communicates essential requirements and functional responsibilities. This revision meets the NIH standard to review a policy every five years.
2. **Filing Instructions:**

Remove: NIH Manual Chapter 1750, dated 08/04/17
Insert: NIH Manual Chapter 1750, dated 10/23/23

PLEASE NOTE: For information on:

- Content of this chapter, contact the issuing office listed above.
- NIH Policy Manual, contact the Division of Compliance Management, Office of Management Assessment (OMA) at 301-496-4606, policymanual@nih.govor refer to 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 (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 ICOs and all NIH staff and contractors.

C. Background

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.

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 the ICO's practices and business processes.

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

D. Policy

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

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. Risk management practices must be considered when designing internal controls and assessing their effectiveness.

The RM Program divides NIH into 38 designated units (NIH access only) for purposes of identifying and reporting on risks. Each designated unit has a Risk Management Officer and Risk Management Champion. The NIH Director, NIH Principal Deputy Director, NIH Deputy Director for Management, ICO Directors, OMA, 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 E 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 Risk Management Guidebook for ICOs 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. ICOs will review available mission-related strategic plan(s) and understand the associated goals and objectives
        ii. ICOs will consider the parameters of operating constraints when planning their risk management activities

    b. Phase #2 - Identify and Score:

i. ICOs will identify and score risks that have the potential to impact the achievement of the ICO's mission, strategic goals, and objectives
ii. ICOs 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 Risk Management Guidebook for ICOs

c. Phase #3 - Assess:

i. ICOs will participate in, and support NIH-wide assessments or special reviews conducted by OMA, as set forth in Section G of this policy
ii. ICOs will conduct internal ICO assessments to adequately manage their internal risks
iii. ICOs 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. ICOs 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 Risk Management Guidebook

e. Phase #5 – Monitor:

i. ICOs 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. ICOs will monitor the status of risk responses
iii. ICOs 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, ICOs should integrate periodic internal ICO assessments as part of management's continuous monitoring of internal controls

f. Phase #6 – Report:

i. ICOs will provide OMA with an annual risk inventory update in the NIH central risk management data repository
ii. Individuals or ICOs designated as owners of NIH ERM risks will provide OMA with periodic status updates when requested
iii. ICOs will provide OMA with a supporting annual FMFIA Statement of Assurance, as set out in Section F of this policy

2. NIH 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. ICOs will ensure that employees who are assigned risk management program roles understand their responsibilities and can execute RM Program requirements.

E. Roles and Responsibilities

1. **NIH Director and Principal Deputy Director** will determine NIH strategic goals and objectives, designate NIH ERM risks and oversee progress on NIH ERM risk management activities.
2. **NIH Office of the Director, Office of Management, Deputy Director for Management** will provide executive sponsorship for the RM Program.
3. **Office of Management Assessment** will 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 G.
4. **ICO Directors** will establish a culture of risk management excellence and integrity within the ICO, determine ICO strategic goals and objectives, designate ICO ERM risks and oversee progress on ICO ERM risk management activities.
5. **Management and Budget Working Group (MBWG)** will serve as the governance body for the NIH RM Program. Periodically, the MBWG will provide the NIH Principal Deputy Director a proposed NIH ERM Risk Profile that identifies the top NIH enterprise risks.
6. **Risk Management Officers** will plan, coordinate, and manage the ICO risk management programs, assess, report on ICO Office internal controls, and facilitate determination and prioritization of ICO ERM risks.
7. **Risk Management Champions** will serve as a liaison between Risk Management Officer, Risk Managers, and OMA and provide risk management support to their Risk Management Officer.
8. **Risk Managers** will ensure compliance with applicable laws, regulations, and policies. Identify, manage, and be accountable for the acceptance of risk, within their functional area. This includes the identification and management of potential fraud risks.
9. **NIH Employees** will 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.

F. 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
3. Reliable financial reporting

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

ICOs will:

1. Provide OMA with an annual Statement of Assurance signed by the ICO 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
4. If deficiencies are identified, manage and facilitate remediation efforts including the development, documentation, implementation, monitoring, and reporting of Corrective Action Plans, in accordance with the HHS Corrective Action Planning: Remediation and Risk Acceptance policy requirements
5. Provide information and documentation to support the Office of Financial Management and the Office of the Chief Information Officer efforts to review internal controls over reporting

G. Internal Control Assessments and Special Management Reviews

OMA supports the vision and research mission of NIH by conducting internal control assessments to identify and leverage program strengths while simultaneously addressing weaknesses, which ensures operations are more efficient and effective, reporting is accurate and reliable, and applicable laws and regulations are being followed. These actions are in line with the Assess phase of the NIH Risk Methodology.

OMA responds to requests from NIH senior leadership concerning identified or perceived risks across the NIH enterprise. When requested, OMA will:

1. Analyze and test internal controls of a program area to determine whether the design and operations are functioning as intended.
2. Disseminate a report detailing enterprise-wide observations and recommendations to the key stakeholders including the NIH Deputy Director for Management.
3. Request from key stakeholders an action plan to address recommendations to implement process improvements. Management must determine whether to accept the risk or remediate deficiencies no later than 60 calendar days after formal communication to the NIH Deputy Director for Management.

4. Collaborate with key stakeholders to monitor and report completion of corrective actions, in compliance with the HHS Policy for Corrective Action Planning. Remediation actions for control deficiencies that do not contribute to a significant deficiency or material weakness shall be implemented at the discretion of the NIH Deputy Director for Management and monitored internally at OMA.

H. 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/Pages/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. HHS Policy "Corrective Action Planning: Remediation and Risk Acceptance", dated February 7, 2023 at Corrective Action Planning - Remediation and Risk Acceptance (February 7, 2023).pdf (nih.gov)
5. Federal Manager's Financial Integrity Act of 1982 at https://www.congress.gov/97/statute/STATUTE-96/STATUTE-96-Pg814.pdf
6. OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (revised), dated July 15, 2016, at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf
7. OMB Circular A-11, Preparation, Submission, and Execution of the Budget, Section 270.2, dated August 2022, at https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf
8. Government Performance and Results Act of 1993 at https://www.congress.gov/103/statute/STATUTE-107/STATUTE-107-Pg285.pdf
9. Government Performance and Results Modernization Act of 2010 at https://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf
10. GAO Standards for Internal Control in the Federal Government, dated September 2014 at http://www.gao.gov/assets/670/665712.pdf
11. GAO Fraud Risk Framework, dated July 2015 at https://www.gao.gov/assets/gao-15-593sp.pdf
12. NIH Manual Chapter 1743 "Managing Federal Records," at https://policymanual.nih.gov/1743
13. Playbook: Enterprise Risk Management for the U.S. Federal Government, dated December 2022 at Enterprise Risk Management Playbook (Fall 2022 Update) (nih.gov)

I. Definitions

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

2. **Enterprise Risks:** 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.
3. **Fraud:** The act of obtaining something of value through willful misrepresentation.
4. **Internal Control:** 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.
5. **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.
6. **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.
7. **Reduction of Risk:** Risk Manager planning and implementing new activities that support or replace current policies, controls, and procedures intended to lessen the likelihood of the risk occurring and/or the impact the risk has on the ICO.
8. **Remediation:** The process where the party responsible for addressing a deficiency corrects a weakness (e.g., develops and implements a corrective action plan) and mitigates the risk(s) associated with the weakness.
9. **Risk:** The possibility that an event or condition, both positive (opportunity) and negative (challenge) may occur that would impact an ICO. All activities at every level of an ICO involve some risk.

Additional supporting guidance is located in the NIH Risk Management Guidebook which can be accessed on the NIH Risk Management Program website.