

# NIH POLICY MANUAL

## 1750 – NIH Risk Management Program

OD/OM/Office of Management Assessment 301-496-1873

Release Date: 04/25/12

---

1. **Explanation of Material Transmitted:** This chapter outlines responsibilities for complying with the NIH Risk Management Program. This revision eliminates the requirement for a mid-year review listed in the previous issue under the Policy section, F.5(b) and its reporting requirements under Policy section F.6(a), as well as updates to hyperlinks.
2. **Filing Instructions:**

**Remove:** NIH Manual Chapter 1750, dated 12/17/09

**Insert:** NIH Manual Chapter 1750, dated 04/25/12

**PLEASE NOTE:** For information on:

- Contents of this chapter, contact the issuing office listed above, or enter this URL: <http://oma.nih.gov/RMAL/NIHRM/default/default.aspx> (NIH Access Only).
  - NIH Manual System, contact the Division of Management Support (DMS), OMA at (301) 496-4606, or enter this URL: <http://oma.od.nih.gov/manualchapters/>
- 

### A. Purpose:

This chapter outlines responsibilities for complying with the NIH Risk Management Program (RM Program). The RM Program establishes and outlines procedures for managing risks and for evaluating controls that improve programs and operations within the agency's extramural, intramural, and administrative components.

## **B. Authority:**

The Federal Manager's Financial Integrity Act (FMFIA) and OMB Circular A-123 require every Federal agency to conduct an annual evaluation of its systems of internal control and to submit an annual report to the President and the Congress on the results of that evaluation and on the adequacy of those systems. The FMFIA directs agencies to use systematic and proactive measures to:

1. develop and implement appropriate, cost effective management controls for results-oriented management,
2. assess the adequacy of internal controls in programs and operations,
3. identify needed improvements, and
4. take corresponding corrective action.

## **C. References:**

1. Federal Manager's Financial Integrity Act of 1982 (P.L. 97-255) at [http://www.whitehouse.gov/omb/financial\\_fmfi1982/](http://www.whitehouse.gov/omb/financial_fmfi1982/)
2. OMB Circular A-123, Management's Responsibility for Internal Control (revised), December 21, 2004 at [http://www.whitehouse.gov/omb/circulars\\_a123\\_rev](http://www.whitehouse.gov/omb/circulars_a123_rev)
3. Government Performance and Results Act (GPRA) of 1993 (P.L. 103-62) at <http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m>
4. Chief Financial Officers' Act (CFO) of 1990 (P.L. 101-576) at <http://www.gao.gov/special.pubs/af12194.pdf> and at [http://www.whitehouse.gov/omb/financial\\_default/](http://www.whitehouse.gov/omb/financial_default/)
5. GAO Standards for Internal Control in the Federal Government, dated November 1, 1999 at <http://www.gao.gov/special.pubs/ai00021p.pdf>
6. OMB Circular A-127, Financial Systems, (revised), January 9, 2009 at [http://www.whitehouse.gov/omb/circulars\\_a127/](http://www.whitehouse.gov/omb/circulars_a127/)

7. Accountability of Tax Dollars Act of 2002 (P.L. 107-289) at [http://www.whitehouse.gov/sites/default/files/omb/assets/about\\_omb/107-2891.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/about_omb/107-2891.pdf)
8. Implementation Guidance for the American Recovery and Reinvestment Act of 2009 at [http://www.whitehouse.gov/omb/assets/memoranda\\_fy2009/m09-15.pdf](http://www.whitehouse.gov/omb/assets/memoranda_fy2009/m09-15.pdf)
9. HHS Guidance Manual for OMB Circular A-123 Assessment at [http://oma.nih.gov/RMAL/NIHRM/default/Shared\\_Documents/2010\\_A-123\\_Guidance\\_Manual\\_-\\_1\\_11\\_10\\_FINAL.pdf](http://oma.nih.gov/RMAL/NIHRM/default/Shared_Documents/2010_A-123_Guidance_Manual_-_1_11_10_FINAL.pdf) (NIH Access Only)
10. NIH Manual Chapter 1743, "Keeping and Destroying Records, Appendix 1, NIH Records Control Schedule" at <http://oma.od.nih.gov/manualchapters/management/1743/>

## **D. Background:**

Risk management is a continuous process carried out by all members of an organization, and is designed to proactively identify and mitigate risks to achieve the organization's objectives, strategy, and mission. Risk management involves identifying, scoring, assessing, remediating, monitoring and reporting organizational risks, and communicating risks throughout an organization. When identifying and assessing risks, mission-based strategic goals and objectives should be considered. These steps form a continuous cycle that is embedded in all of the organization's practices and business processes.

## **E. Roles and Responsibilities:**

In-depth descriptions of each role and responsibility can be found in the [NIH Risk Management Guidebook \(Guidebook\)](#) (NIH Access Only). Additional roles and responsibilities are also defined in the Guidebook, including that of the governance structure.

1. **Assessable Unit (AU)** – An AU is a discrete subset of a mission-oriented organization. AUs may exist at various levels throughout the agency. However, for purposes of this policy, each Institute and Center and designated OD Offices each will be an AU to meet the goals and objectives of the NIH RM Program. A list of the NIH AUs is available on

the OMA website at <http://oma.nih.gov/RMAL/NIHRM/default/Shared%20Documents/Organizational%20Framework.aspx> (NIH Access Only).

2. **NIH Director** – The NIH Director is the Agency Risk Owner (ARO). The NIH Director takes ultimate ownership of the full set of risks facing the organization. The NIH Director also:
  - a. sponsors the RM Program,
  - b. establishes support of a risk management culture within NIH through agency-wide communications,
  - c. holds senior officials accountable for risk management, and
  - d. provides the final NIH FMFIA Statement of Assurance to the Department of Health and Human Services.
3. **Risk Owners (RO)** – IC Directors and designated OD Office Directors serve as the ROs for their AUs. The RO:
  - a. implements and maintains a risk management program within his or her organization,
  - b. appoints the Risk Management Officer,
  - c. owns all risks identified within their organization, and
  - d. signs and submits an annual FMFIA Statement of Assurance to the NIH Director.
4. **Deputy Director for Management (DDM)** – The DDM is responsible for the overall NIH Risk Management Program, FMFIA reporting, and ensuring that reasonable and adequate controls are in place to protect NIH resources from fraud, waste, abuse and mismanagement. The DDM also makes the final determination of material weaknesses for purposes of the FMFIA report.
5. **Risk Management Officers (RMO)** – Each AU has a Risk Management Officer (RMO) to lead their risk management activities. RMOs are

responsible for seeing that risk management activities within their AUs are being conducted effectively. Executive Officers typically fill this role, as do certain designated OD Office Directors. The RMO:

- a. determines the AU risk management structure, associated Risk Managers and Risk Management Champion,
- b. serves as the primary point of contact regarding RM Program activities,
- c. coordinates with the Risk Managers and other subject matter experts to identify, score and validate risks, and
- d. assesses the adequacy of internal controls to reasonably assure that the AU and NIH can collectively achieve stated missions.

6. **Risk Managers (RM)** – RMs are selected based on the risk management structure at the AU. The RM:

- a. identifies, scores and manages risks within his/her functional area that impact the AU mission and NIH mission,
- b. proposes appropriate risk responses to identified risks, and
- c. develops corrective action plans (CAPs) to address control gaps and deficiencies.

7. **Risk Management Champion (RMCh)** – A Risk Management Champion (RMCh) is an individual responsible for executing the day-to-day activities to facilitate the RM Program and provide support to the RMO. In general, the “Champion” should have a thorough knowledge and familiarity of the AU’s mission, challenges, and personnel.

8. **Office of Management Assessment (OMA)** – The NIH OMA is responsible for facilitating RM Program activities at the agency level and providing guidance to the AUs for establishing and managing risk management programs within their organizations.

## **F. Policy:**

All employees are responsible for risk management. The NIH Director, IC Directors, designated Risk Management Officers (RMO), Risk Management Champions (RMCh), and Risk Managers (RM), are responsible for implementing and maintaining risk management programs and reinforcing a culture of risk management and accountability. To support the program, NIH will maintain a governance structure consisting of senior leaders from across the organization to oversee RM Program activities at the agency level. The NIH RM Methodology as well as roles and responsibilities associated with each phase of the RM Methodology are outlined in the Guidebook at

<http://oma.nih.gov/RMAL/NIHRM/default/Shared%20Documents/RM%20Guidebook%203.0%20-%20FINAL.pdf> (NIH Access Only).

Working through their respective RMOs, AUs will:

1. Organize the risk management process (RM Methodology Phase #1):
  - a. AUs will establish their own internal risk management structure, and
  - b. AUs will implement the RM Program using the prescribed tools, processes and procedures outlined in the Guidebook.
2. Identify and score risks (RM Methodology Phase #2):
  - a. AUs will provide to OMA all identified risks that have the potential to significantly impact the achievement of the AU and NIH missions, and
  - b. AUs will routinely monitor their risk environment and identify and score new risks, review existing risks for continued applicability, and rescore risks based on current circumstances.
3. Assess controls associated with identified risks (RM Methodology Phase #3):
  - a. AUs will participate in and support control assessments conducted by OMA for prioritized risks selected from the NIH risk inventory,
  - b. AUs will conduct control assessments to adequately manage its individual risks, and

- c. AUs will notify OMA immediately upon determination of a potential material weakness as defined within the OMB Circular A-123, Management's Responsibility for Internal Controls (revised) December 21, 2004. OMA will notify the DDM of potential material weaknesses.
4. Manage, mitigate and remediate risks as appropriate (RM Methodology Phase #4):
  - a. AUs will update and document policies and procedures,
  - b. AUs will incorporate reasonable controls into procedures, programs and operations,
  - c. AUs will propose a risk response to identified risks and document the reasoning for such response, and
  - d. AUs will develop corrective action plans (CAPs) that are approved by the RMO, and executed to mitigate or remediate risks.
5. Monitor risks and controls continuously (RM Methodology Phase #5):
  - a. AUs will monitor the status of all outstanding CAPs to ensure accurate and timely completion, and
  - b. AUs 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 regular assigned duties of personnel. In addition, periodic assessments should be integrated as part of management's continuous monitoring of internal control.
6. Ensure that periodic risk management reports are provided to relevant internal and external stakeholders (RM Methodology Phase #6):
  - a. AUs will provide OMA with an annual inventory update that summarizes the reassessment of the AU's risk inventory.
7. Use risk management data for decision-making:

- a. AUs will use risk management data as an integral part of the decision-making process at all levels within NIH, and
  - b. AUs will maintain documentation that supports the rationale for management decisions involving significant risks.
8. AUs should input RM Program activities into the NIH central risk management data repository. Authorized users can access the system at <http://nbsgrcmprod.nih.gov:22080/oraclegrcmanager/nav/frame.aspx>
  9. AUs will ensure that employees and staff responsible for risk management activities are trained. The Guidebook provides a detailed explanation of each phase of the NIH RM Methodology, as well as the roles and responsibilities associated with each phase. The most current Guidebook is available on the OMA website at <http://oma.nih.gov/RMAL/NIHRM/default/Shared%20Documents/RM%20Guidebook%203.0%20-%20FINAL.pdf> (NIH Access Only).

## **G. FMFIA:**

NIH management is responsible for establishing and maintaining effective internal control and financial management systems that meet the objectives of the FMFIA and Office of Management and Budget (OMB) Circular A-123. These objectives are to ensure 1) effective and efficient operations, 2) compliance with applicable laws and regulations, and 3) reliable financial reporting. As required by OMB Circular A-123, NIH is required to evaluate its internal controls and financial management systems to determine whether these objectives are being met. As such, AUs must be able to provide annual assurance to the NIH Director that their controls are operating effectively.

Working through their respective RMOs, AUs will:

1. submit timely Annual FMFIA Statements of Assurance,
2. provide supporting data as requested, to prepare the NIH Preliminary and Final FMFIA Statement of Assurance Reports,
3. provide an annual Statement of Assurance signed by the IC Director and designated OD Office Director, and an Assurance Statement Support

- Summary outlining risk management activities for the current fiscal year,
4. maintain documentation supporting their annual Statement of Assurance,
  5. conduct internal control reviews within their organization to ensure internal controls are operating effectively and efficiently, and
  6. provide information and documentation to support the Office of Financial Management efforts to review internal controls over financial reporting.

## **H. Special Studies and Reviews:**

Periodically, the OMA is directed to perform internal control or management reviews of NIH Institutes and Centers. As directed by the NIH Director, Principal Deputy Director or through a Congressional request, OMA will:

1. perform ad-hoc internal control or management reviews,
2. provide a copy of the Draft Internal Control or Management Review Report to the subject of the review for comment on findings and recommendations, and
3. disseminate a Final Internal Control or Management Review Report to the NIH Director and Principal Deputy Director upon finalizing the review.

## **I. Definitions:**

See Appendix

## **J. Records Retention and Disposal:**

All records (e-mail and non-e-mail) pertaining to this chapter must be retained and disposed of under the authority of NIH Manual 1743, Keeping and Destroying Records, Section 1700 ' Management Services: "1700-A-12 (a – f) Management Control Records". Refer to the NIH Chapter for specific disposition instructions at

<http://oma.od.nih.gov/manualchapters/management/1743/1700.html>.

NIH e-mail messages, including attachments that are created on NIH computer systems or transmitted over NIH networks that are evidence of the activities of

the agency or have informational value are considered Federal records. These records must be maintained in accordance with current NIH Records Management guidelines.

All e-mail messages are considered Government property, and, if requested for a legitimate Government purpose, must be provided to the requester. Employees' supervisors, NIH staff conducting official reviews or investigations, and the Office of Inspector General may request access to or copies of the e-mail messages. All e-mail messages must also be provided to Congressional oversight committees if requested and are subject to Freedom of Information Act requests. Back-up files are subject to the same requests as the original messages.

## **K. Internal Controls:**

The purpose of this manual issuance is to outline responsibilities for complying with the NIH Risk Management Program.

1. **The Office Responsible for Reviewing Internal Controls Relative to this Chapter:** Office of Management Assessment, NIH.
2. **Frequency of Review:** Ongoing review.
3. **Method of Review:** An overall agency-wide evaluation of compliance with this policy, including conducting periodic reviews of AU risk management activities.
4. **Review Reports:** Review reports are sent to the affected IC and OD Directors, Risk Management Officers, and to the Director, Office of Management Assessment.

## **Appendix: Definitions**

**Assessable Unit (AU):** An assessable unit is a discrete subset of a mission-oriented organization. AUs may exist at various levels throughout the agency. However, for purposes of this policy, each Institute and Center and designated OD Offices each will be an AU to meet the goals and objectives of the NIH RM Program. Each designated AU has a Risk Management Officer (RMO) to lead their risk management activities.

**AU Risk Inventory:** An AU risk inventory is a portfolio of AU risks that serves as a reference for further AU risk management activities.

**Control:** A control is (1) a mechanism to prevent or reduce the likelihood of a risk occurring, and (2) an activity to reduce the impact of a risk should it occur.

**Control Assessment:** A control assessment evaluates the effectiveness of the processes and controls associated with an identified risk.

**Corrective Action Plan (CAP):** A corrective action plan is a detailed plan outlining the intended activities to mitigate a risk.

**NIH Risk Inventory:** The NIH risk inventory is an agency-wide portfolio of risks that serves as a reference for further risk management activities.

**NIH Risk Management Methodology (RM Methodology):** The NIH Risk Management Methodology is a customized six-phase approach that provides a standardized means of addressing risks at NIH.

**NIH Risk Management Program (RM Program):** The NIH RM Program is an ongoing process to perform standardized repeatable activities that promote the overall efficiency, effectiveness, accountability and integrity of the organization's work.

**Risk:** A risk is the possibility that an uncertain event or condition may occur that would negatively impact an organization.

**Risk Management Data:** Risk management information will provide NIH management with additional data to consider in budget decision-making, as well as greater insight on the risk inventory and control activities to improve operations.

**Risk Management Structure:** A risk management structure is a segmentation of an AU to facilitate risk management activities.

**Risk Response:** A risk response is an action to align risk impact and risk likelihood within an organization's tolerance for risk.

[Manual Chapters Main Menu](#)

[Browse](#)

[Search](#)

[Back to OMA Home Page](#)

---

[NIH](#)