U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 4.4	ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL	DT-23-04
Volume 4:	Financial Management	
Approved By:	James C. Corbett Acting Chief Financial Officer	
Date Approved:	April 3, 2023	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Financial Officer Division of Budget	
Contact Name:	David Holley	

EXECUTIVE SUMMARY

Management Directive 4.4, "Enterprise Risk Management and Internal Control," is revised to help ensure the U.S. Nuclear Regulatory Commission complies with—

- The Federal Managers' Financial Integrity Act of 1982;
- Office of Management and Budget Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control" requirements; and
- Government Accountability Office, "Standards for Internal Control in the Federal Government" (Green Book) requirements.

In addition, the NRC has revised this management directive as part of its efforts to use more inclusive language in its publications. These changes, which include changing "Chairman" to "Chair" in some instances, are purely editorial and do not affect the meaning of the guidance in this document.

TABLE OF CONTENTS

I. POLICY 2

II. OBJECTIVES 2

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY 3

A. Chair 3

B. Chief Financial Officer (CFO) 3

C. Executive Director for Operations (EDO) 4
D. Inspector General (IG) 5
E. General Counsel (GC) 5
F. Performance Improvement Officer (PIO) 5
G. Executive Committee on Enterprise Risk Management (ECERM) 6
H. Programmatic Senior Assessment Team (PSAT) 6
I. Senior Assessment Team (SAT) 6
J. Office Directors and Regional Administrators 6
IV. APPLICABILITY **8**
V. DIRECTIVE HANDBOOK **8**
VI. REFERENCES **8**

I. POLICY

The U.S. Nuclear Regulatory Commission (NRC) is mandated by the Federal Managers' Financial Integrity Act of 1982 (FMFIA or the Integrity Act) to establish and maintain effective internal control. The Office of Management and Budget (OMB) Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," requires agencies to implement an enterprise risk management (ERM) capability coordinated with the strategic planning and strategic review process established by the Government Performance and Results Act Modernization Act (GPRAMA), and the internal control processes required by the Integrity Act and the Government Accountability Office's (GAO), "Standards for Internal Control in the Federal Government" (Green Book).

II. OBJECTIVES

- Establish an ERM governance and communications structure that identifies risks and challenges early, and brings them to the attention of the appropriate level of agency leadership to develop effective solutions.
- Integrate ERM into the agency's performance management and internal control frameworks to improve mission delivery, reduce costs, and focus corrective actions towards key enterprise risks.

– Provide policy guidance that ensures reasonable assurance that—

- Agency programs are achieving their intended results, and are protected from waste, fraud, abuse, and mismanagement;
- Resources are being used consistent with the agency's mission;
- Information systems are authorized and appropriately secured;
- Laws and regulations are followed; and
- Reliable and timely information is obtained, maintained, reported, and used for sound decision-making.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Chair

1. Signs the agency's annual Integrity Act Statement, which is sent to OMB and Congress.
2. Appoints the Chief Financial Officer (CFO).

B. Chief Financial Officer (CFO)

1. Provides executive oversight over the agency's financial resources with respect to ERM.
2. Provides review to ensure the completion of the internal control assessment process specifically related to the reporting and data, as defined by OMB Circular A-123, Appendix A, "Management of Reporting and Data Integrity Risk," and OMB Circular A-123, Appendix C, "Requirements for Payment Integrity Improvement."
3. Chairs the Senior Assessment Team (SAT), which is responsible for providing strategic direction for the internal control assessment process specifically related to financial reporting and financial systems.
4. Co-chairs the Executive Committee on Enterprise Risk Management (ECERM), the NRC senior management council, which sets the agency's strategic direction for internal control, assesses and monitors deficiencies in internal control, and makes a recommendation to the Chair annually on whether to sign the agency's Integrity Act Statement.
5. Ensures that the NRC's financial systems comply with Federal financial system requirements, applicable Federal accounting standards, and the U.S. Treasury standard general ledger at the transaction level, as required by the Federal Financial Management Improvement Act (FFMIA) of 1996.

6. Leads and coordinates the development of the annual Agency Financial Report in accordance with the requirements of OMB Circular A-136, "Financial Reporting Requirements."
7. Approves and signs the annual Statement of Assurance on internal control over reporting, as a subset of management assurance statements stipulated by OMB Circular A-123 and the Integrity Act.
8. Issues jointly with the Executive Director for Operations (EDO) the annual memorandum, "Fiscal Year XX ERM, Programmatic Internal Control, and Reasonable Assurance Guidance," which can be found at the following link: Reasonable Assurance Guidance.
9. Certifies reasonable assurance for the Financial Management and Policy Support Product Lines.
10. Leads the agency's reasonable assurance certification process.
11. Informs the agency of any enterprisewide risks and risk mitigation efforts concerning the Financial Management and Policy Support Product lines.

C. Executive Director for Operations (EDO)

1. Serves as the Chief Operating Officer (COO), as designated by the Chair and defined by the GPRAMA.
2. Provides executive oversight of and the leads the agency's ERM processes, including the development of the agency's risk appetite and the Executive Performance Management System, which includes the Quarterly Performance Review (QPR) Dashboard and agency risk profile.
3. Serves as the agency's lead to provide overall management to monitor and improve agency performance and achieve the agency's mission and goals through the use of strategic and performance planning, measurement, analysis, and regular assessment of performance information.
4. Appoints the agency Performance Improvement Officer (PIO) and Chief Information Officer (CIO), who report to the EDO.
5. Co-chairs the ECERM, which is the NRC senior management council that sets the agency's strategic direction for internal control, assesses and monitors deficiencies in internal control, and makes a recommendation to the Chair annually on whether to sign the agency's Integrity Act Statement.
6. Leads QPR meetings to review and discuss the Programmatic Senior Assessment Team's (PSAT) evaluation of enterprise risks and mitigation strategies.

7. Oversees the CIO's maintenance of the agency's comprehensive framework for ensuring the effectiveness of information security controls over automated information resources in support of NRC assets and financial operations.
8. Jointly, with the CFO, issues ERM, programmatic internal control, and reasonable assurance guidance.
9. Promotes the application and execution of enterprise risk management practices in the strategic planning, performance planning, and reporting processes.
10. Serves as the agency's Office of the Inspector General (OIG) and GAO liaison.

D. Inspector General (IG)

1. Oversees independent audits and investigations regarding possible violations of law, fraud, waste, abuse, and mismanagement based on the mandates of the Inspector General Act.
2. Serves as an advisory member of the ECERM.
3. Maintains independence from the ECERM's decision-making process.

E. General Counsel (GC)

1. Serves as an advisory member of the ECERM.
2. Provides independent advice and legal counsel to the Chair, Commission, EDO, CFO, and ECERM.

F. Performance Improvement Officer (PIO)

1. Leads the agency's performance management program.
2. Leads and coordinates the systematic development of the agency's Annual Performance Plan and the Annual Performance Report in accordance with GPRAMA requirements.
3. Chairs the agency's Performance Improvement Panel (PIP) and establishes and maintains the PIP charter.
4. Supports the EDO and Deputy Executive Directors for Operations (DEDOs) in the review of agency performance, including the review and approval of enterprise risks as identified by the PSAT.
5. Ensures that enterprise risks are communicated to the Chair, Commission, ECERM, PIP, and other appropriate entities.
6. Reviews and approves agency risks to be discussed at the QPR meetings.

G. Executive Committee on Enterprise Risk Management (ECERM)

1. Provides strategic oversight over all NRC programs and organizations.
2. Reviews business line annual reasonable assurance certifications.
3. Ensures that the focus areas (agencywide risks identified by PSAT through the QPR meetings including the results from the fourth quarter of the fiscal year to address OIG Audit 21-A-16 Recommendation 7) stated in the Reasonable Assurance Justification Document (RAJD) have been addressed by mitigation strategies/solutions to ensure the agency meets its mission, strategic goals, and objectives.
4. Votes annually on a recommendation to the Chair on the state of Internal Control.

H. Programmatic Senior Assessment Team (PSAT)

1. Documents business line risks and communicates enterprisewide risks to OEDO for review and discussion at the QPR meetings.
2. Develops mitigation strategies for identified risks and communicates the strategies to the ECERM at the QPR meetings.

I. Senior Assessment Team (SAT)

1. Provides strategic oversight and direction for NRC's internal control review process, specifically related to the assessment of effectiveness of internal control over reporting and data quality, as required by OMB Circular A-123, Appendix A and Appendix C.
2. Approves the Statement of Assurance to be included in the annual Agency Financial Report.

J. Office Directors and Regional Administrators

1. General

   (a) Manage the performance of their daily operations to ensure programs function efficiently and effectively. For the purposes of programmatic internal control and reasonable assurance, the EDO and CFO have chosen to treat the corporate support product lines and the international activities product line as business lines.

   (b) Coordinate and delegate, as appropriate, work assignments and project management, ensuring that interdependencies that may exist among offices are

addressed and clearly communicated to office directors, regional administrators, and key staff.

(c) Coordinate cross-cutting issues, consistent with ECERM and Office of the Chief Financial Officer guidance, with other organizational units to increase the likelihood of achieving intended outcomes, and reduce the likelihood and impact of potential risks.

2. Business Line Leads (BLL)

(a) As members of the PSAT, communicate enterprise risks, from their business lines to the ECERM at the QPR meetings. Document business line risks in the QPR Dashboard for OEDO review, per instructions in OEDO Procedure 0960, "Enterprise Risk Management Reporting Instructions" (ML19161A125).

(b) Monitor the implementation and outcomes of business line internal control plan activities throughout the fiscal year, as needed, and ensure programs are managed efficiently and effectively.

(c) Document controls and procedures followed as part of the agency's annual reasonable assurance certification process.

(d) Certify reasonable assurance for the business line.

(e) Corporate support product lines and the International Activities product line are treated as business lines for the purpose of reasonable assurance.

3. Product Line Leads (PLL)

(a) Provide support to meet the established outcomes of product line internal control plan activities throughout the fiscal year, as needed, and ensure programs are managed efficiently and effectively.

(b) Document controls and procedures followed as part of the agency's annual reasonable assurance certification process.

(c) Product Lines can either be programmatic such as International Activities or corporate such as the Financial Management Product Line.

(d) Product Lines are treated as a business line for Internal Control Memorandums of Understanding (MOUs) and Reasonable Assurance processes only.

(e) Certify reasonable assurance for the product line.

4. Partner Office Leads

(a) For those business lines in which they participate, ensure an effective control environment to facilitate the offices meeting their missions.

(b) Coordinate and communicate with their business line leads, where appropriate, to ensure that interdependencies that may exist among offices are addressed and clearly communicated to ensure complexities and risks are mitigated, and programs are managed efficiently and effectively.

(c) Document controls and procedures followed, and make that documentation available as part of the agency's internal control program and annual reasonable assurance certification process.

IV. APPLICABILITY

This MD is intended to assist the staff in maintaining effective risk management and internal control. The policies in this MD apply to all NRC employees in headquarters and regional offices, and to all mission activities. NRC managers, supervisors, and staff at all levels are responsible for active participation in achieving the objectives of this MD. Along with MD 4.4, the NRC leverages its QPR process, as described in MD 6.9, "Performance Management," to address OIG Audit 21-A-16 Recommendation 6(d).

V. DIRECTIVE HANDBOOK

Handbook 4.4 provides guidance for the agency's implementation of ERM and internal control.

VI. REFERENCES

Nuclear Regulatory Commission

Annual NRC Memorandum, "Fiscal Year XX Enterprise Risk Management, Programmatic Internal Control, and Reasonable Assurance Guidance," available in ADAMS at https://adamsxt.nrc.gov/navigator/bookmark.jsp?desktop=ADAMS&repositoryId=MainLibrary&repositoryType=p8&docid=Folder%2C%7BFADD9FBE-4595-43E6-B85B-8F2B7707A2E9%7D%2C%7BDD1534E1-3B22-4ED0-B670-22F486907AF0%7D&mimeType=folder&template_name=Folder.

Executive Performance Management System SharePoint site, https://usnrc.sharepoint.com/teams/edo-epms/SitePages/Home.aspx.

Management Directive 6.9, "Performance Management."

Management Directive 6.10, "Strategic Planning."

OEDO Procedure 0960, "Enterprise Risk Management Reporting Instructions."

Office of Management and Budget

OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control."

Appendix A, "Management of Reporting and Data Integrity Risk."

Appendix B, "A Risk Management Framework for Government Charge Card Programs."

Appendix C, "Requirements for Payment Integrity Improvement."

Appendix D, "Compliance with the Federal Financial Management Improvement Act of 1996."

OMB Circular A-136, "Financial Reporting Requirements."

United States Code

Accountability of Tax Dollars Act of 2002 (Pub. L. 107-289).

Chief Financial Officers Act of 1990, as amended (Pub. L. 101-576).

Clinger-Cohen Act of 1996 (Pub. L. 104-106).

Federal Financial Management Improvement Act of 1996 (Pub. L. 104-208).

Federal Managers' Financial Integrity Act of 1982 (Pub. L. 97-255).

Government Performance and Results Act Modernization Act of 2010 (Pub. L. 111-352).

Inspector General Act of 1978, as amended (5 U.S.C. §§ 401–424).

Miscellaneous

Charters—

Performance Improvement Panel (ML17030A124).

Programmatic Senior Assessment Team (ML16067A159).

Senior Assessment Team (ML22304A205).

Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Internal Control – Integrated Framework."

Government Accountability Office, "Standards for Internal Control in the Federal Government" (Green Book), available at https://www.gao/products/gao-14-704g.

U.S. NUCLEAR REGULATORY COMMISSION DIRECTIVE HANDBOOK (DH)

DH 4.4	ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL	DT-23-04
Volume 4:	Financial Management	
Approved By:	James C. Corbett Acting Chief Financial Officer	
Date Approved:	April 3, 2023	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Financial Officer Division of Budget	
Contact Name:	David Holley	

EXECUTIVE SUMMARY

Management Directive 4.4, "Enterprise Risk Management and Internal Control," is being revised to help ensure the U.S. Nuclear Regulatory Commission complies with—

- The Federal Managers' Financial Integrity Act of 1982;
- Office of Management and Budget Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control" requirements; and
- Government Accountability Office, "Standards for Internal Control in the Federal Government" (Green Book) requirements.

In addition, the NRC has revised this management directive as part of its efforts to use more inclusive language in its publications. These changes, which include changing "Chairman" to "Chair" in some instances, are purely editorial and do not affect the meaning of the guidance in this document.

TABLE OF CONTENTS

I. OVERVIEW OF THIS HANDBOOK 2

A. Purpose of This Handbook 2

B. Roadmap 3

II. ENTERPRISE RISK MANAGEMENT 3

A. Overview 3

B. Governance 4

C. Risk Profiles 6
III. NRC INTERNAL CONTROL OVER PROGRAMMATIC OPERATIONS 7
A. Overview 7
B. Government Accountability Office (GAO) Standards for Internal Control 10
C. Internal Control Plan (ICP) 13
D. Internal Control Memorandums of Understanding (MOUs) 13
E. Internal Control Process and Requirements Catalog 13
F. Training 13
IV. COMPLIANCE WITH OMB CIRCULAR A-123 APPENDICES 14
A. OMB Circular A-123, Appendix A Assessment 14
B. OMB Circular A-123, Appendix C Assessment 15
V. REASONABLE ASSURANCE CERTIFICATIONS AND AGENCY STATEMENT OF ASSURANCE 15
A. Overview 15
B. Business Line (BLLs and PLLs) Reasonable Assurance Certification 15
C. Executive Committee on Enterprise Risk Management (ECERM) 16
D. Agency Integrity Act Statement 16
VI. GLOSSARY 17

FIGURES

Figure 1. ERM and the NRC Mission 5
Figure 2. Risk Hierarchy 7
Figure 3. NRC's Federal Managers' Financial Integrity Act of 1982 (FMFIA) Governance Framework 8
Figure 4. NRC Programmatic Internal Control Program 9
Figure 5. OMB A-123 Appendix A Workflow 14

I. OVERVIEW OF THIS HANDBOOK

A. Purpose of This Handbook

Handbook 4.4 describes the general framework for how the agency complies with the Federal Managers' Financial Integrity Act of 1982 (FMFIA or Integrity Act), Office of

Management and Budget (OMB) Circular A-123, and the Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government (Green Book). Annual internal control and reasonable assurance guidance is issued jointly by the Chief Financial Officer (CFO) and the Executive Director for Operations (EDO), and is located in the Agencywide Documents Access and Management System (ADAMS).

B. Roadmap

This handbook addresses four performance and compliance areas.

1. Enterprise Risk Management (ERM). This section provides an overview of the enterprisewide approach for risk management at the U.S. Nuclear Regulatory Commission (NRC).
2. Internal Control over Programmatic Operations. This section discusses the importance of internal control in the Federal Government, agency-specific roles and responsibilities, and an overview of the agency's internal control program.
3. Compliance with OMB Circular A-123 appendices. This section discusses the agency's adherence to Appendix A of OMB Circular A-123, "Management of Reporting and Data Integrity Risk," and Appendix C of OMB Circular A-123, "Requirements for Payment Integrity Improvement."
4. Reasonable Assurance Certifications and Agency Integrity Act Statement. This section explains the preparation of reasonable assurance certifications, and the agency's Integrity Act Statement.

II. ENTERPRISE RISK MANAGEMENT

ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides better insight about how to most effectively prioritize resource allocations to ensure successful mission delivery.

Office of Management and Budget Circular A-123

A. Overview

1. The Office of the Chief Financial Officer (OCFO) developed the agency's ERM Framework (ADAMS ML16328A168), which leverages existing agency practices, governance organizations and programs, and communications channels while adhering to guidance established by OMB Circular A-123. Federal best practices suggest the following key components must be shared for successful implementation, which the NRC has incorporated into its ERM framework:

(a) A structured approach to understanding and managing risk;

(b) Senior leadership buy-in and trust in establishing acceptable risk tolerance levels, as well as sharing risk information across the agency (effective risk management cannot be managed in silos); and

(c) An appreciation that risk can create opportunities to improve current practices.

2. The applicability of ERM in the Federal sector will evolve as lessons-learned and best practices continue to be shared among Federal ERM practitioners and OMB. The NRC will continually incorporate best practices, as appropriate, in efforts to mature its ERM framework.

B. Governance

1. The Office of the Executive Director for Operations (OEDO), with the support of the agency's Programmatic Senior Assessment Team (PSAT), is primarily responsible for the agency meeting ERM requirements. All senior leaders, including the Performance Improvement Officer (PIO) and members of the PSAT are responsible for ensuring the agency becomes and remains a modern, risk-informed regulator.

2. Business Line Leads (BLLs), Product Line Leads (PLLs), and partner office leads are responsible for identifying and managing risks in their respective areas and communicating appropriately those risks that could impact them in accomplishing their strategic objectives, or the agency meeting its mission.

3. All agency employees and contractors are encouraged to be open, candid, and fact-based in discussing risk, making all relevant facts and information available so leadership can make risk-informed decisions.

4. ERM and its relationship to the NRC mission is illustrated in Figure 1. Management is responsible for ensuring that appropriate controls are in place to ensure the effectiveness and efficiency of agency operations. Risk management is a series of coordinated activities to direct and control challenges or threats to achieving an organization's goals and objectives. ERM ensures that a portfolio view of agency risk is available to the executive leadership for appropriate decision-making. Internal control, risk management, and ERM are all part of the overall Governance process. In addition, the agency leverages its Quarterly Performance Review (QPR) processes, as described in MD 6.9, "Performance Management," and its governance framework outlined in Section II of this handbook. This approach to integrating and focusing on ERM and internal control enables the agency to identify and prioritize risks, including those at the business/product line level and those that span across organizations to address OIG Audit OIG-21-A-16, recommendation 6(d).

Figure 1. ERM and the NRC Mission

C. Risk Profiles

> **Risk profiles are a prioritized inventory of the most significant risks identified from a portfolio perspective.**
>
> ***Office of Management and Budget Circular A-123***

1. In accordance with OMB Circular A-123, agencies must maintain a risk profile. The primary purpose of a risk profile is to provide a thoughtful analysis of the risk an agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risk. In the context of the NRC, a risk profile is an analysis of the risk (risk is defined as an event or situation that, if it occurs, will negatively impact the NRC's assets, activities, or operations) the agency faces in achieving its strategic objectives, and the identification of appropriate options for addressing those risks. The risk profile assists in facilitating a determination around the aggregate level and types of risks that the agency and its management are willing to assume to achieve its strategic objectives. The agency's risk profile can be found on the OEDO Executive Performance Management System SharePoint site.
2. The agency leverages its QPR process as a mechanism for the PSAT, composed of the BLLs and PLLs, to document and communicate enterprisewide risks. The OEDO issues ERM Reporting Instructions (ML19161A125) and provides support to the BLLs and PLLs on appropriately documenting risks, including assessing the likelihood of occurrence, evaluating the impact, and mitigating strategies.
3. Figure 2 demonstrates the hierarchical methodology used in developing the agency's risk profile. The BLLs and PLLs identify their risks and document them for the QPR meetings. The PIO, and Executive Committee on Enterprise Risk Management (ECERM) are responsible for prioritizing those risks that are deemed significant enough to impact the agency's ability to meet its mission or the goals and objectives as stated in the Strategic Plan. Those risks ascend to the agency's risk profile to address OIG Audit OIG-21-A-16, recommendation 2(a). All other risks are managed at the business line and product line levels.

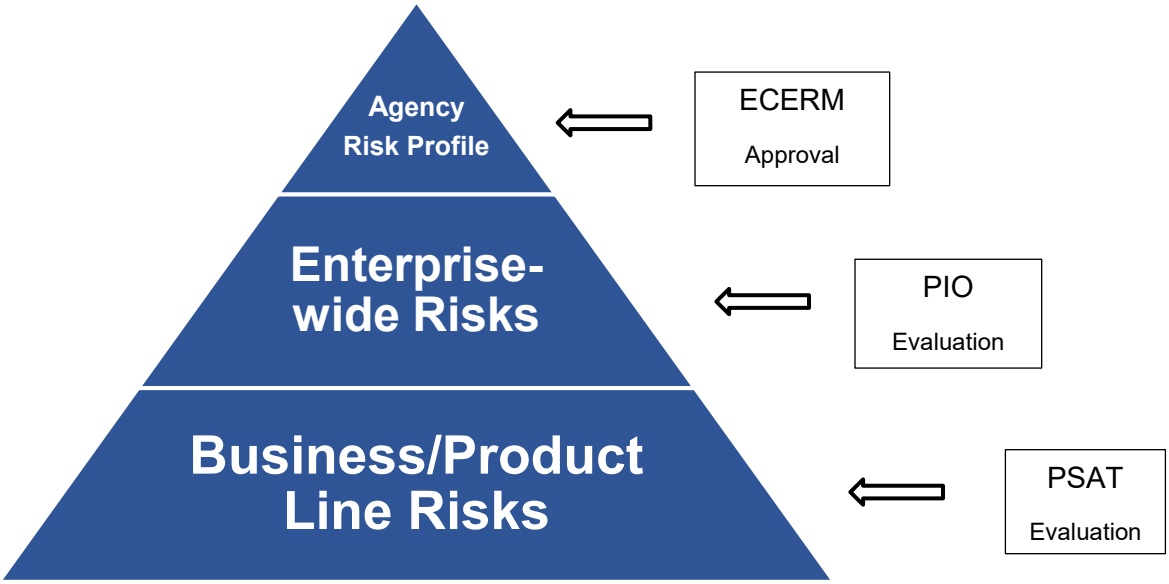


Figure 2. Risk Hierarchy

Internal Control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved.

Government Accountability Office's Green Book

III. NRC INTERNAL CONTROL OVER PROGRAMMATIC OPERATIONS

A. Overview

1. FMFIA requires the NRC to establish and maintain an effective internal control program and annually report to the President and Congress on the effectiveness of the program. OCFO, as the lead for establishing and maintaining an internal control program for NRC programmatic and administrative activities, partners with OEDO and the agency's BLLs and PLLs, and partner offices to ensure the agency meets FMFIA requirements.

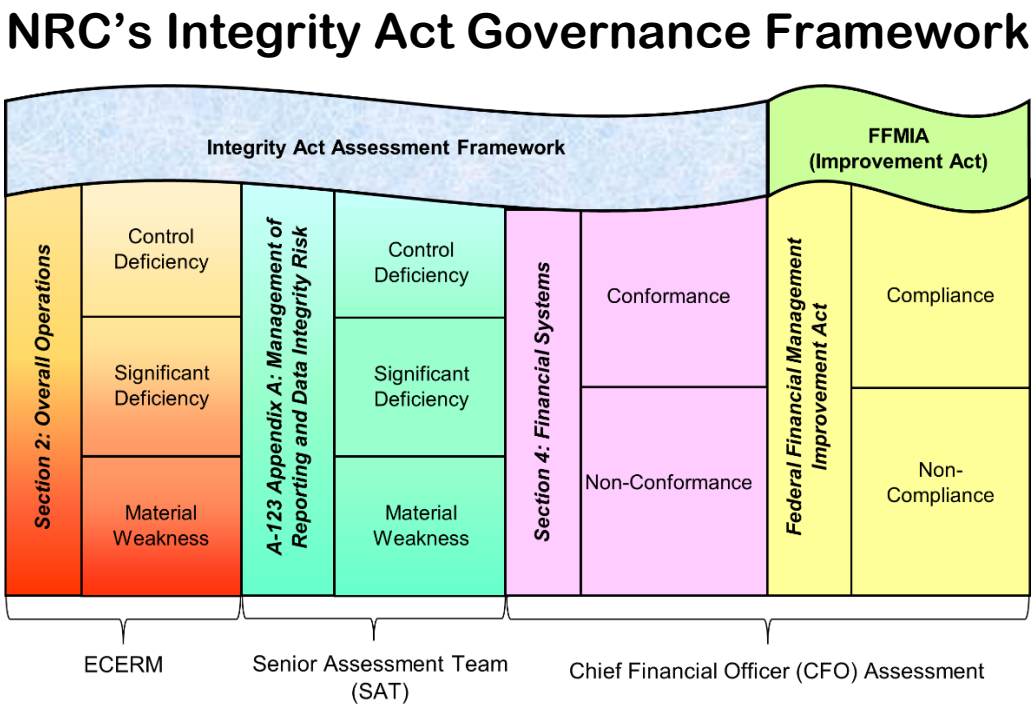
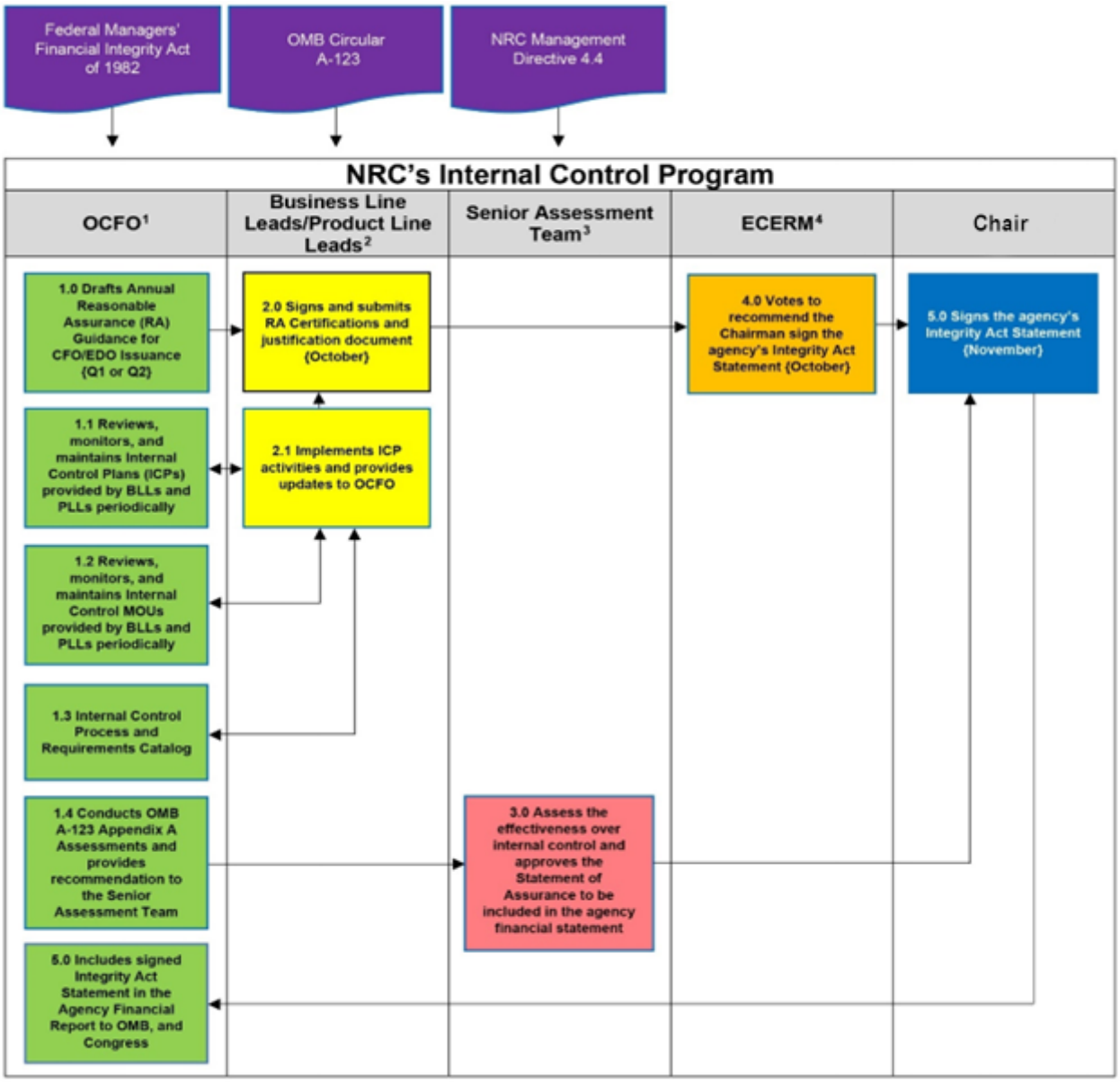


Figure 3. NRC's Federal Managers' Financial Integrity Act of 1982 (FMFIA) Governance Framework

2. Figure 3 is a graphical representation of the NRC's FMFIA framework. Reading Figure 3 from right to left: the CFO is responsible for ensuring the agency complies with the Federal Financial Management Improvement Act of 1996 (FFMIA), and Section 4 of FMFIA, "Financial Systems." The Senior Assessment Team (SAT), chaired by the CFO, is responsible for ensuring the agency complies with Appendix A of OMB Circular A-123. The ECERM, co-chaired by the CFO and the EDO, is responsible for ensuring that the agency's internal control over programmatic operations complies with FMFIA.

3. OCFO's Internal Control Team coordinates the agency's reasonable assurance certification process, serves as liaisons between the CFO and BLLs/PLLs and partner offices, and provides technical expertise, guidance, training, and administration for compliance with FMFIA. For the purpose of this handbook, Figure 4 provides an overview of internal control activities that provide reasonable assurance that controls are in place, and are being followed and used for appropriate decision-making.

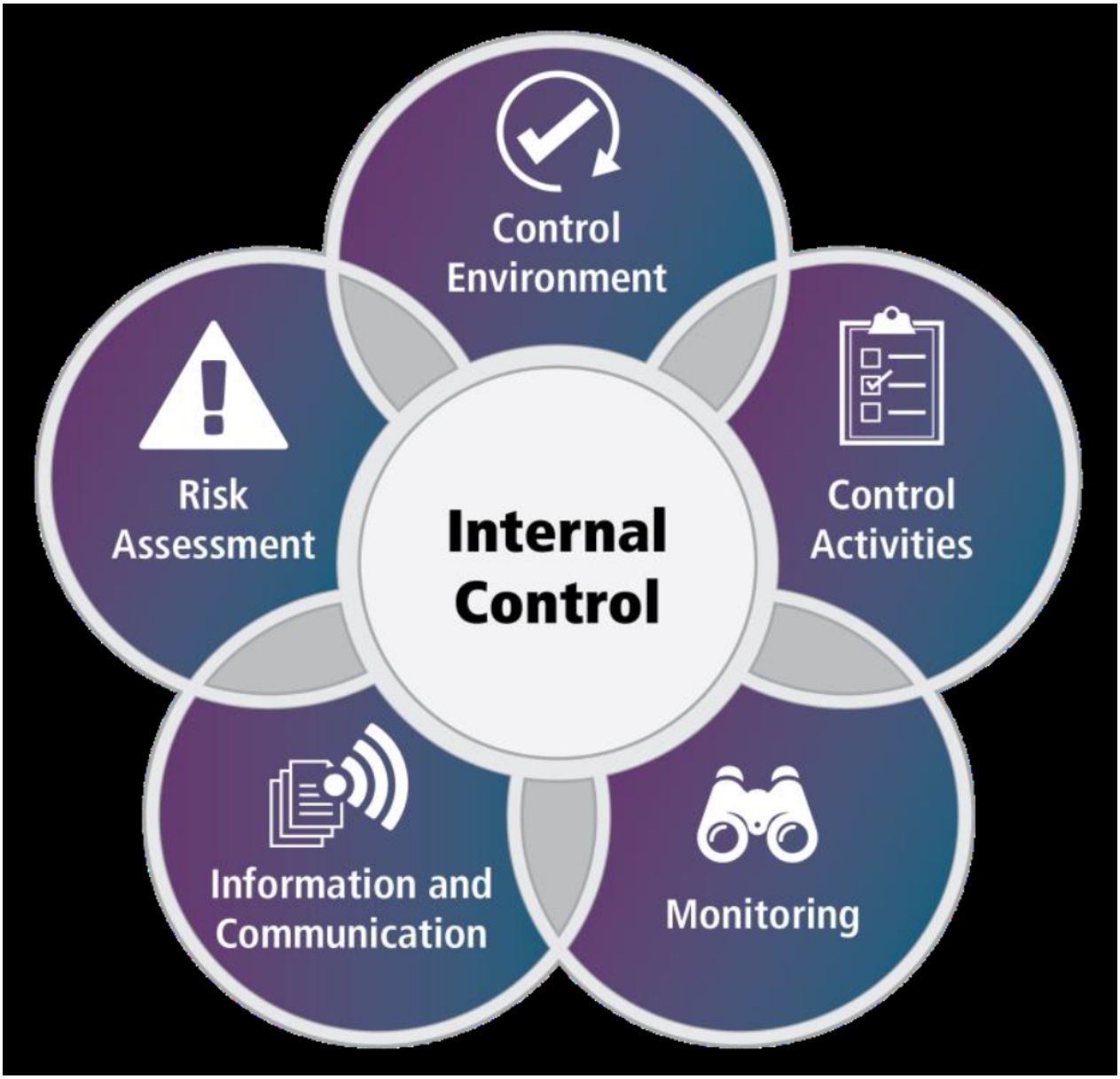
Figure 4. NRC Programmatic Internal Control Program



[1] OCFO administers the Programmatic Internal Control Program and Reasonable Assurance Certification processes and supports the business lines and product lines as applicable per Internal Control Team deliverables throughout the year.
[2] NRC Business Line Lead and Product Line Lead is the senior executive (office director) of the respective lines.
[3] Chaired by the Chief Financial Officer and is responsible for providing strategic direction for the internal control assessment process specifically related to financial reporting and financial systems under OMB Circular A-123 Appendix A.
[4] The ECERM is co-chaired by the agency's Executive Director for Operations and the Chief Financial Officer. Members of the ECERM are comprised of senior executives from the Office of the Executive Director for Operations, with the agency's General Counsel and Inspector General serving as advisory members.

B. Government Accountability Office (GAO) Standards for Internal Control

1. To help agencies comply with the requirements of the FMFIA, GAO established standards for effective internal control in the Federal Government. These standards apply to all aspects of agency operations and provide the basis by which internal control is evaluated.



2. For the purpose of plain language and applicability to the NRC, the five components that the GAO uses to define the principles of internal control are as follows:

   (a) **Control Environment:** The foundation for all other standards. It provides the discipline and structure, which affect the overall quality of the internal control. It influences how objectives are defined and how control activities are structured. Members of an oversight body understand the entity's objectives, risks, and expectations to stakeholders. Management, with oversight from the oversight body, defines the organization's expectations of ethical values in the standards of conduct. Examples include strategic planning, safety culture climate, ethics program, and management directives and other internal policies. The five principles of this component are—

      (i) Principle 1 – The oversight body and management should demonstrate a commitment to integrity and ethical values.

      (ii) Principle 2 – The oversight body should oversee the entity's internal control system.

      (iii) Principle 3 – Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

      (iv) Principle 4 – Management should demonstrate a commitment to recruit, develop and retain competent individuals.

      (v) Principle 5 – Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

   (b) **Risk Assessment:** Upon establishing an effective control environment, management assesses the risk facing the entity as it seeks to achieve its objectives. Assessment provides the basis for developing appropriate risk responses from risks stemming from both external and internal resources. The four principles of this component are—

      (i) Principle 6 – Management should define objectives clearly to enable the identification of risks and define risk tolerances.

      (ii) Principle 7 – Management should identify, analyze, and respond to risks related to achieving the defined objectives.

      (iii) Principle 8 – Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

      (iv) Principle 9 – Management should identify, analyze, and respond to significant changes that could impact the internal control systems.

(c) **Control Activities: Proactive and corrective** actions taken by management to help ensure objectives are achieved and mitigation of risks are appropriate. Examples include proper segregation of duties, physical controls over assets, rulemakings, inspections, access restrictions to and accountability for resources and records, reviews by management at the functional or activity level, establishment of performance measures and indicators, proper execution of transactions, etc. The three principles of this component are—

(i) Principle 10 – Management should design control activities to achieve objectives and respond to risks.

(ii) Principle 11 – Management should design entity's information system and related control activities to achieve objectives and respond to risks.

(iii) Principle 12 – Management should implement control activities through policies.

(d) **Information and Communication:** Management uses quality information to support the internal control system. Effective information and communication are vital for an entity to achieve its objectives. Examples include Staff Requirements Memoranda, SECY papers, yellow announcements, and public meetings. The three principles of this component are—

(i) Principle 13 – Management should use quality information to achieve the entity's objectives.

(ii) Principle 14 – Management should internally communicate the necessary quality information to achieve the entity's objectives.

(iii) Principle 15 – Management should externally communicate the necessary quality information to achieve the entity's objectives.

(e) **Monitoring:** A continuous process of observing the internal control system to ensure internal control remains aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the quality of performance over time and promptly resolves the findings of audits and other reviews. Examples include the reactor and fuel cycle oversight programs and the agency executive leadership and advisory councils. The two principles of this component are—

(i) Principle 16 – Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

(ii) Principle 17 – Management should remediate identified internal control deficiencies on a timely basis.

C. Internal Control Plan (ICP)

Each NRC BLL and PLL shall develop the Internal Control Plan (ICP) for their business line or product line. Internal control ensures the effectiveness and efficiency of operations, the integrity of financial and accounting information, and the resolution of deficiencies. Lack of internal control can result in program deficiencies, which could impact an agency's ability to meet its mission, strategic goals, and objectives. The ICP "is the foundation for documenting internal control activities" per the Audit of NRC's Reactor Business Lines' Compliance with Agency Non-Financial Internal Control Guidance (OIG-15-A-16). Based on GAO's Green Book, the ICP objectives are classified by the following three categories.

1. Operations – Effectiveness and efficiency of operations.
2. Reporting – Reliability of reporting for internal and external use.
3. Compliance – Compliance with applicable laws and regulations.

D. Internal Control Memorandums of Understanding (MOUs)

The purpose of Internal Control Memorandums of Understanding (MOUs) is to identify, clarify, and communicate mutual mission expectations as they relate to internal control and reasonable assurance certification. The MOUs are a part of the documentation for the agency's annual certification by management of reasonable assurance over Internal Control.

E. Internal Control Process and Requirements Catalog

The NRC Internal Control Requirements &Processes Catalog is a centralized repository of requirements and processes documentation used by agency officials in the conduct of their work. The catalog documents requirements and processes pertaining to program effectiveness, operations, communications, and laws and regulations. This catalog is also a part of the documentation for the agency's annual certification by management of reasonable assurance over Internal Control.

F. Training

The course, "Internal Control - A Path Forward to Accountability" (available in TMS), is awareness training designed to introduce key ERM and Internal Control concepts and external requirements to all NRC staff. This training is mandatory for all agency employees and new hires.

IV. COMPLIANCE WITH OMB CIRCULAR A-123 APPENDICES

Management is responsible for evaluating whether a system of internal control reduces the risk of not achieving the entity's objectives related to operations, reporting, or compliance to an acceptable level. In evaluating internal control, management should follow a risk-based assessment approach.

Office of Management and Budget Circular A-123

A. OMB Circular A-123, Appendix A Assessment

1. OMB Circular A-123, Appendix A, "Management of Reporting and Data Integrity Risk," provides requirements related to obtaining reasonable assurance over reporting. Appendix A allows agencies the flexibility to assess, document, and report on the effectiveness of internal controls that have been designed and implemented to mitigate risks over significant reporting and data integrity used by management for decision-making.
2. OCFO has adopted a phased workflow to complete the Appendix A assessment, as shown below in Figure 5. OCFO, along with SAT strategic oversight, will use the NRC's Enterprise Risk Management process to evaluate risk and test internal controls to only those reporting objectives where inaccurate, unreliable, or outstanding reporting would significantly impact the agency's ability to accomplish its mission and performance goals or objectives. Once the risk assessment and testing are concluded, OCFO provides the results of any internal control and process improvement recommendations to the SAT to support the annual reasonable assurance certification.

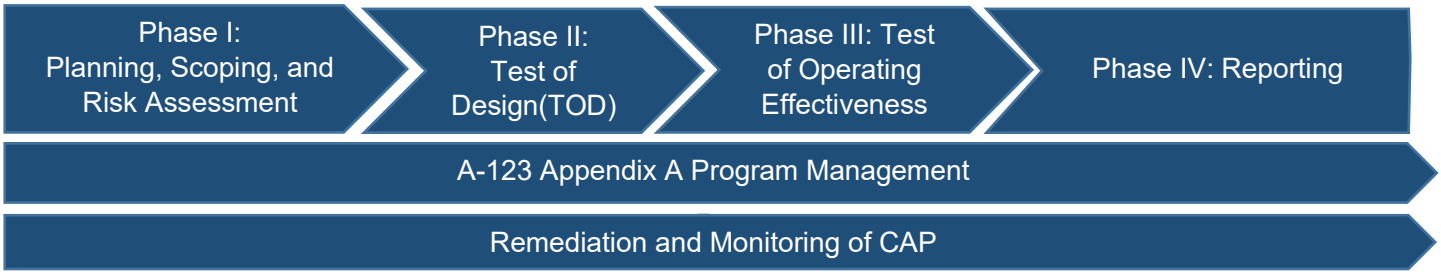


Figure 5. OMB A-123 Appendix A Workflow

B. OMB Circular A-123, Appendix C Assessment

OMB Circular A-123, Appendix C, "Requirements for Payment Integrity Improvement" provides requirements for agencies to determine compliance with the Payment Integrity Information Act of 2019 (PIIA) (Public Law 116-117). OCFO conducts a triannual assessment to identify and review all programs that meet the statutory threshold of PIIA to determine susceptibility to significant improper payments. OCFO conducts a quantitative and qualitative risk assessment of all programs to determine susceptibility and testing requirements. The SAT identified commercial payments, grants payments, employee payments, payroll, and Government charge cards as program areas to test, pending results of the PIIA risk assessment. Should any programs be identified as being susceptible, the NRC will initiate the process to fully implement the requirements of PIIA and to report on actions taken, or plans to take, to recover improper payments and prevent future improper payments. In addition, the NRC conducts additional risk assessments, as needed, if there are material changes in program operations or if the NRC establishes new programs. The results and recommendations of the triannual assessment will be presented to the SAT and documented in the Agency Financial Report (AFR).

V. REASONABLE ASSURANCE CERTIFICATIONS AND AGENCY STATEMENT OF ASSURANCE

> **The Statement of Assurance represents the agency head's informed judgment as to the overall adequacy and effectiveness of internal control within the Agency related to operations, reporting, and compliance.**
>
> ***Office of Management and Budget Circular A-123***

A. Overview

FMFIA requires the NRC to submit a Statement of Assurance as of September 30 of each fiscal year, on the state of the agency's internal control over programmatic operations and financial reporting, also referred to as the Integrity Act Statement, which is signed by the Chair, and published in the AFR.

B. Business Line (BLLs and PLLs) Reasonable Assurance Certification

1. NRC office directors and regional administrators are responsible for concurring on the Agency's Reasonable Assurance Justification Document (RAJD), which provides supporting documentation that the NRC has adequate internal controls in place over compliance, operations, and reporting to accomplish its mission. RAJD provides hyperlinks to QPR data to include ERM Risk Reports and agencywide internal control documentation. The ERM implementation activities through the QPR process

leads to the ERM focus areas and the reporting of ERM in the Integrity Act statement to address OIG Audit OIG-21-A-16, recommendation 6(b).

2. The partner offices are responsible for accomplishing their missions, and supporting the BLLs/PLLs in conducting their operations in a manner that allows them to certify reasonable assurance.

3. The BLLs/PLLs certify that there is reasonable assurance that internal control over operations, reporting, and compliance is adequate to achieve the following objectives:

   (a) Program Management – Programs are achieving their intended results, and are protected from waste, fraud, abuse, and mismanagement;

   (b) Resource Management – Resources are being used consistently with the agency's mission;

   (c) IT Systems – Information systems are authorized and appropriately secured;

   (d) Laws and Regulations – Laws and regulations are followed; and

   (e) Communication – Reliable and timely information is obtained, maintained, reported, and used for sound decision-making.

C. Executive Committee on Enterprise Risk Management (ECERM)

At the end of the fiscal year, including the results of the fourth quarter of the fiscal year to address OIG Audit OIG-21-A-16, recommendation 7, the ECERM assesses the agency's programmatic operations, financial systems, and internal control over reporting. The ECERM reports to the NRC Chair if there are any internal control deficiencies that are serious enough to require reporting as a material weakness or significant deficiency. The ECERM makes a recommendation to the Chair to sign the agency's Integrity Act Statement.

D. Agency Integrity Act Statement

The Chair signs the agency's Integrity Act Statement, which is submitted to OMB and Congress. The Chair's signature indicates that NRC senior leadership has evaluated the status of its internal control, reporting processes, and financial systems, in accordance with the Integrity Act and the FFMIA, and either confirms or denies reasonable assurance that the NRC internal control achieves its intended results.

VI. GLOSSARY

Agency Financial Report (AFR)

An annual report submitted by the head of the agency to OMB and the Congress within 45 days after the end of the fiscal year. The report provides financial and performance results. The AFR summarizes the agency's mission, activities, program and financial performance, systems, controls, legal compliance, financial position, and financial condition.

Control Deficiency

A control deficiency exists when the design, implementation, or operation of control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risk. Although it does not meet the criteria of a material weakness or significant deficiency, it must be corrected to prevent the possible occurrence of waste, loss, unauthorized use, or misappropriation.

Executive Committee on Enterprise Risk Management (ECERM)

The NRC senior management council, chaired by the CFO and co-chaired by the EDO, whose membership includes senior agency managers, that is responsible for assessing, monitoring, and providing oversight and strategic direction for agency programmatic internal control.

Material Weakness

A reportable condition that the agency head determines is significant enough to report outside of the agency.

Programmatic Senior Assessment Team (PSAT)

An Internal Control governance body consisting of BLLs and PLLs responsible for ensuring their programmatic and financial operations are functioning in the most effective and efficient manner possible, in accordance with the Integrity Act, OMB Circular A-123, and GAO's Green Book. They are also responsible for elevating significant business line- and product line-level risks to the enterprisewide level to the ECERM for discussion and analysis at the QPR meetings.

Reasonable Assurance

A managerial decision, based on available information, that the internal control in place provides a satisfactory level of confidence that internal control objectives will be met. The standard of reasonable assurance prescribed by OMB and GAO recognizes that the cost of internal control should not exceed the benefits derived and that errors or irregularities

may occur and go undetected because of inherent limitations in internal control resulting from resource constraints, statutory and regulatory restrictions, and other factors.

Reasonable Assurance Certification

An annual statement of assurance that summarizes, as of September 30, the business lines' and product lines' compliance with the requirements of the Integrity Act and OMB Circular A-123.

Reasonable Assurance Justification Document

A document that supports NRC's assertion that it has adequate internal controls in place to accomplish its mission.

Risk

An event or situation that, if it occurs, will negatively impact the NRC's assets, activities, or operations.

Senior Assessment Team (SAT)

The SAT is chaired by the CFO. The membership includes the Deputy CFO, Comptroller, Budget Director, OCFO Internal Team Leader, and the office directors from the Office of the Chief Information Officer, the Office of Administration, and the Office of the Chief Human Capital Officer. The SAT reviews and approves the A-123, Appendix A assessment process, and approves internal control over the annual Statement of Assurance.

Significant Deficiency

A deficiency or a combination of deficiencies in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

Statement of Assurance (Integrity Act Statement)

An annual statement required by the Integrity Act that represents the Chair's informed judgment as to the overall adequacy and effectiveness of internal control within the agency. The statement reports the results of evaluations made on the agency's system of controls over programmatic operations, financial and non-financial reporting, information technology and information management, and compliance with applicable laws based upon a fiscal year, October 1 through September 30.