

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

MD 4.4	ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL	DT-17-18
<i>Volume 4:</i>	Financial Management	
<i>Approved By:</i>	Maureen E. Wylie Chief Financial Officer	
<i>Date Approved:</i>	December 14, 2017	
<i>Cert. Date:</i>	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog .	
<i>Issuing Office:</i>	Office of the Chief Financial Officer Division of Planning and Budget	
<i>Contact Name:</i>	David Holley	
EXECUTIVE SUMMARY		
<p>Management Directive (MD) 4.4, “Enterprise Risk Management and Internal Control,” is being issued to help ensure the U.S. Nuclear Regulatory Commission complies with—</p> <ul style="list-style-type: none"> • 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. <p>MD 4.4 has been retitled from “Internal Control” to “Enterprise Risk Management and Internal Control” and provides high-level policy guidance for reasonable assurance that agency programs achieve their intended results, and that the agency has an appropriate risk management methodology in place to identify risks, to bring them to the attention of the appropriate level of leadership, and to develop effective solutions.</p>		

TABLE OF CONTENTS

I. POLICY	2
II. OBJECTIVES	2
III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY	3
A. Chairman	3

For updates or revisions to policies contained in this MD that were published after the MD was signed, please see the Yellow Announcement to Management Directive index ([YA-to-MD index](#)).

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) (Formerly the Executive Committee for Internal Control)	6
H. Programmatic Senior Assessment Team (PSAT)	6
I. Senior Assessment Team (SAT)	6
J. Office Directors and Regional Administrators	7
IV. APPLICABILITY	8
V. DIRECTIVE HANDBOOK	8
VI. REFERENCES	8

I. POLICY

The U.S. Nuclear Regulatory Commission is mandated by the Federal Managers' Financial Integrity Act of 1982 (FMFIA or the Integrity Act) with the responsibility 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 decisionmaking.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Chairman

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 of, and the lead for, the agency’s ERM, internal control, and reasonable assurance processes.
2. Provides review and oversight of the internal control review, monitoring, and testing of financial management, reporting, and system processes and procedures as defined by OMB Circular A-123, Appendix A, “Internal Control over Financial Reporting.”
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 Chairman 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 financial reporting, as a subset of management assurance statements stipulated by OMB Circular A-123 and FMFIA.
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 product line.
10. Provides guidance to help the NRC develop a common vision, definition, and strategy for establishing and maintaining an enterprise risk management and internal control framework.
11. Provides guidance and coordination to business lines in the updates to the Internal Control Plans.
12. Provides support and technical assistance for the agency's reasonable assurance process.
13. Works with OEDO to ensure that enterprisewide risks are appropriately documented, monitored, and tracked on the agency's risk profile.

C. Executive Director for Operations (EDO)

1. Serves as the Chief Operating Officer (COO), as designated by the Chairman and defined by the GPRAMA.
2. 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.
3. Appoints the agency Performance Improvement Officer (PIO) and the Chief Information Officer (CIO), who report to the EDO.
4. 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 Chairman annually on whether to sign the agency's Integrity Act Statement.

5. Leads quarterly performance review meetings (QPR) to review progress on the agency's business line performance plans, including the Programmatic Senior Assessment Team's (PSAT) evaluation of any enterprise risks as part of the agency's risk profile.
6. 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.
7. Issues jointly with the CFO, annual ERM, programmatic internal control, and reasonable assurance guidance.
8. Promotes the application and execution of enterprise risk management practices in the strategic planning, performance planning, and reporting processes.
9. Ensures that significant enterprisewide risks are appropriately documented, monitored, and tracked on the agency's risk profile in accordance with applicable OMB requirements, and communicated to the Chairman, Commission, ECERM, and other appropriate entities.
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 decisionmaking process.

E. General Counsel (GC)

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

F. Performance Improvement Officer (PIO)

1. Serves as the agency's lead for the performance management program.
2. Leads and coordinates the systematic development of the Annual Performance Plan and the Annual Performance Report in accordance with GPRAMA requirements for all NRC offices.

3. Serves as the chair of the NRC Performance Improvement Panel (PIP) and establishes the PIP charter.
4. Supports the EDO and Deputy Executive Directors for Operations (DEDOs) in the conduct of quarterly review of agency performance, including the review and approval of enterprisewide risks as identified by the PSAT.
5. Ensures that enterprisewide risks are communicated to the Chairman, Commission, EDO, DEDOs, PIP, and other appropriate entities.
6. Collaborates with the CFO through review of certification and supporting documentation.
7. Reviews and approves agencywide risks to be discussed at the quarterly QPR meetings for the risk profile.
8. Determines whether any agencywide risks meet the level of inclusion in a risk profile.

G. Executive Committee on Enterprise Risk Management (ECERM) (Formerly the Executive Committee for Internal Control)

1. Provides strategic oversight over all NRC programs and organizations, which includes assessing and monitoring agency programmatic operations and financial internal control.
2. Reviews business line reasonable assurance certifications.
3. Makes a recommendation to the Chairman annually on the state of Internal Control and ERM.

H. Programmatic Senior Assessment Team (PSAT)

1. Provides oversight to NRC's enterprise risk management and internal control processes in collaboration with the EDO, CFO, and ECERM.
2. Communicates risks that are agencywide and/or of strategic interest from the business line/product line level to the enterprisewide level at the QPR meetings.

I. Senior Assessment Team (SAT)

1. Provides strategic oversight and direction for the internal control assessment process, specifically related to financial reporting and financial systems, as required by OMB Circular A-123, Appendix A.
2. Reviews and recommends CFO signature on the annual Statement of Assurance on internal control over financial reporting, as a subset of Management Assurance Statements stipulated by OMB Circular A-123 and the Integrity Act.

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 as business lines, similar to the programmatic 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 OCFO guidance, with other organizational units to increase the likelihood of achieving intended outcomes.

2. Business Line Leads (BLL)

- (a) As members of the PSAT, communicate major accomplishments, and risks, from the business/product line-level to the enterprisewide-level at the QPR meetings.
- (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.

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) 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 provide the documentation to the business line leads as part of the agency's annual reasonable assurance certification process.

IV. APPLICABILITY

MD 4.4 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.

V. DIRECTIVE HANDBOOK

Handbook 4.4 provides guidance for the NRC implementation of ERM and internal control.

VI. REFERENCES

Nuclear Regulatory Commission

Annual NRC Memorandum, "Fiscal Year XX ERM, Programmatic Internal Control, and Reasonable Assurance Guidance," available in ADAMS at [Reasonable Assurance Guidance](#).

Management Directives

6.9, "Performance Management."

6.10, "Strategic Planning."

Office of Management and Budget

OMB Circular A-11, "Preparation, Submission and Execution of the Budget."

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

Appendix A, "Internal Control over Financial Reporting."

Appendix B, "Improving the Management of Government Charge Card Programs."

Appendix C, “Requirements for effective measurement and Remediation of Improper Payments.”

OMB Circular A-136, “Financial Reporting Requirements” (annually).

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. App.).

Miscellaneous

Charters—

Programmatic Senior Assessment Team:

http://fusion.nrc.gov/ocfo/team/ocfo_admin/dpba/icpb/IC/Documents/.

Senior Assessment Team:

http://fusion.nrc.gov/ocfo/team/ocfo_admin/DOC/.

Performance Improvement Panel:

<http://fusion.nrc.gov/edo/team/CPM/PerfMgmt/FY2017/Shared%20Documents/>.

Chief Financial Officers Council, “Playbook: Enterprise Risk Management for the U.S. Federal Government.”

Enterprise Risk Management Quarterly Performance Review Instructions and Template:

<http://fusion.nrc.gov/edo/team/CPM/PerfMgmt/FY2017/Shared%20Documents/>.

Government Accountability Office, “Standards for Internal Control in the Federal Government” (Green Book).

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

DH 4.4	ENTERPRISE RISK MANAGEMENT AND INTERNAL CONTROL	DT-17-18
---------------	--	-----------------

Volume 4:	Financial Management
Approved By:	Maureen E. Wylie Chief Financial Officer
Date Approved:	December 14, 2017
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 Planning and Budget
Contact Name:	David Holley

EXECUTIVE SUMMARY

Management Directive (MD) 4.4, “Enterprise Risk Management and Internal Control,” is being issued 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.

MD 4.4 has been retitled from “Internal Control” to “Enterprise Risk Management and Internal Control” and provides high-level policy guidance for reasonable assurance that agency programs achieve their intended results, and that the agency has an appropriate risk management methodology in place to identify risks, to bring them to the attention of the appropriate level of leadership, and to develop effective solutions.

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

For updates or revisions to policies contained in this MD that were published after the MD was signed, please see the Yellow Announcement to Management Directive index ([YA-to-MD index](#)).

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).....	10
D. Training	11
IV. NRC INTERNAL CONTROL OVER FINANCIAL REPORTING	11
V. REASONABLE ASSURANCE CERTIFICATIONS AND AGENCY STATEMENT OF ASSURANCE	12
A. Overview	12
B. Business Line (BLLs and PLLs) Reasonable Assurance Certification.....	12
C. Executive Committee on Enterprise Risk Management (ECERM)	12
D. Agency Statement of Assurance (Integrity Act Statement).....	12
VI. DEFINITIONS	13

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

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 of risk management at the U.S. Nuclear Regulatory Commission.
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. Internal Control over Financial Reporting. This section discusses the agency's adherence to Appendix A of OMB Circular A-123, "Internal Control Over Financial Reporting."
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 and the CFO Council. Federal best practices suggest the following key components must be shared for successful implementation, which 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, the CFO Council, and OMB. The NRC will monitor these developments and incorporate them, as appropriate, in updating and enhancing the agency's ERM framework and practices.

B. Governance

1. The CFO, with the support of the EDO, is primarily responsible for the agency meeting ERM requirements. All NRC senior leadership, including the Performance Improvement Officer (PIO) and members of the Programmatic Senior Assessment Team (PSAT), are responsible for encouraging a risk identification culture that promotes accountability and strategic risk management at all levels of the organization.
2. Business line leads (BLLs) and partner office leads have the responsibility to manage risks in their respective areas and communicate appropriately the risks that could impact them in meeting their mission, or could have a broader impact on the agency as a whole.
3. All NRC employees are encouraged to be open, candid, and fact-based in discussing risk issues, 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 decisionmaking. Internal control, risk management, and ERM are all part of the overall Governance process.



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.
2. The NRC leverages the agency's existing Quarterly Performance Review (QPR) process as a mechanism for the PSAT, composed of the BLLs, to document and communicate enterprisewide risks. The Office of the Executive Director for Operations (OEDO), in collaboration with OCFO, issues guidance (see Section VI, "References," Enterprise Risk Management Quarterly Performance Review Instructions and Template) and provides support to the BLLs on appropriately documenting risks, including assessing the likelihood of occurrence, evaluating the impact, and mitigating strategies. It is at the discretion of the CFO, in collaboration with the PIO and the Executive Committee on Enterprise Risk Management (ECERM), to establish the agency's risk tolerance that is used in the agency's risk profile. Currently, OMB requires the agency's risk profile to be finalized and updated annually in June.
3. Figure 2 demonstrates the hierarchical methodology used in developing the agency's risk profile. The BLLs identify their risks and document them for the QPR meetings. The CFO, PIO, and 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, available for submission to OMB upon request. All other risks are managed at the business line and product line levels.

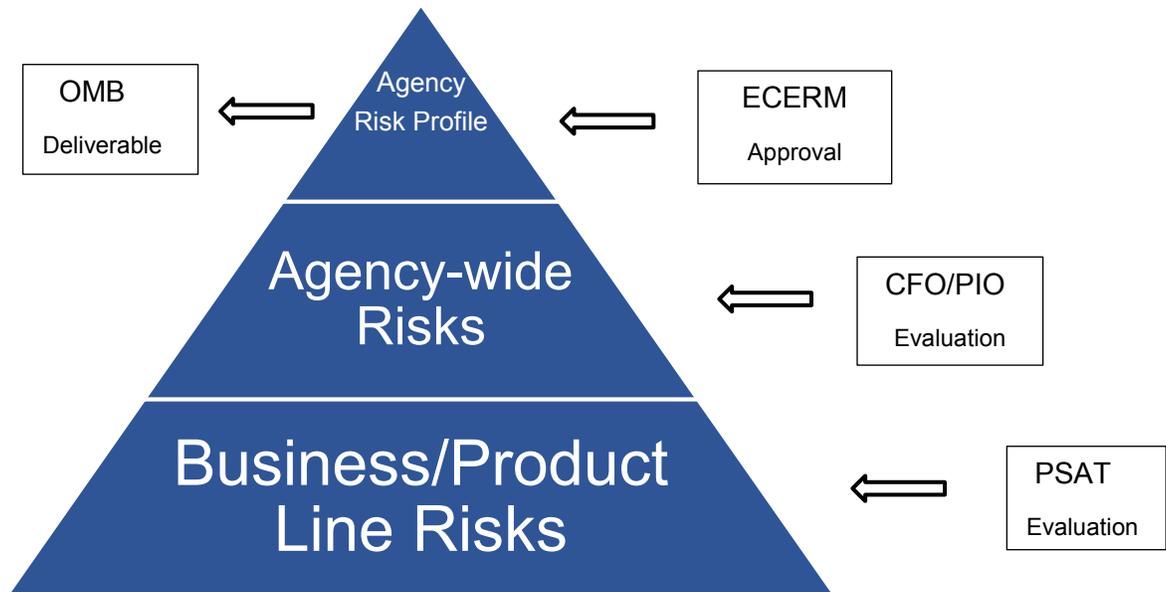


Figure 2. Risk Hierarchy

III. NRC INTERNAL CONTROL OVER PROGRAMMATIC OPERATIONS

“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.”

General Accountability Office’s Green Book

A. Overview

1. The Federal Managers’ Financial Integrity Act of 1982 (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 to ensure the agency meets FMFIA requirements.

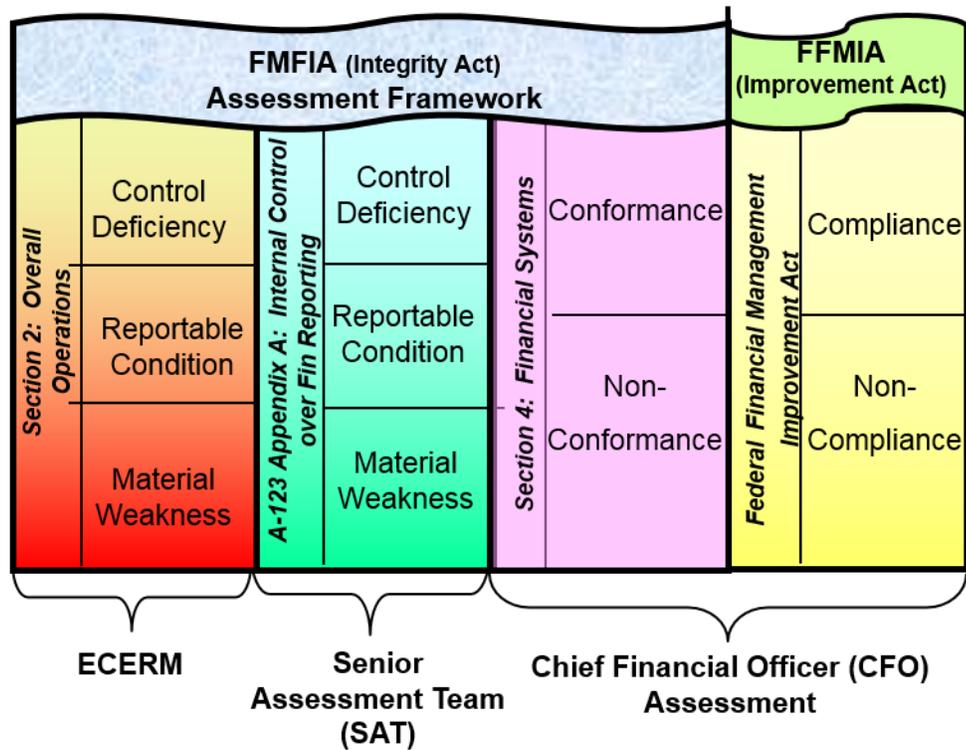
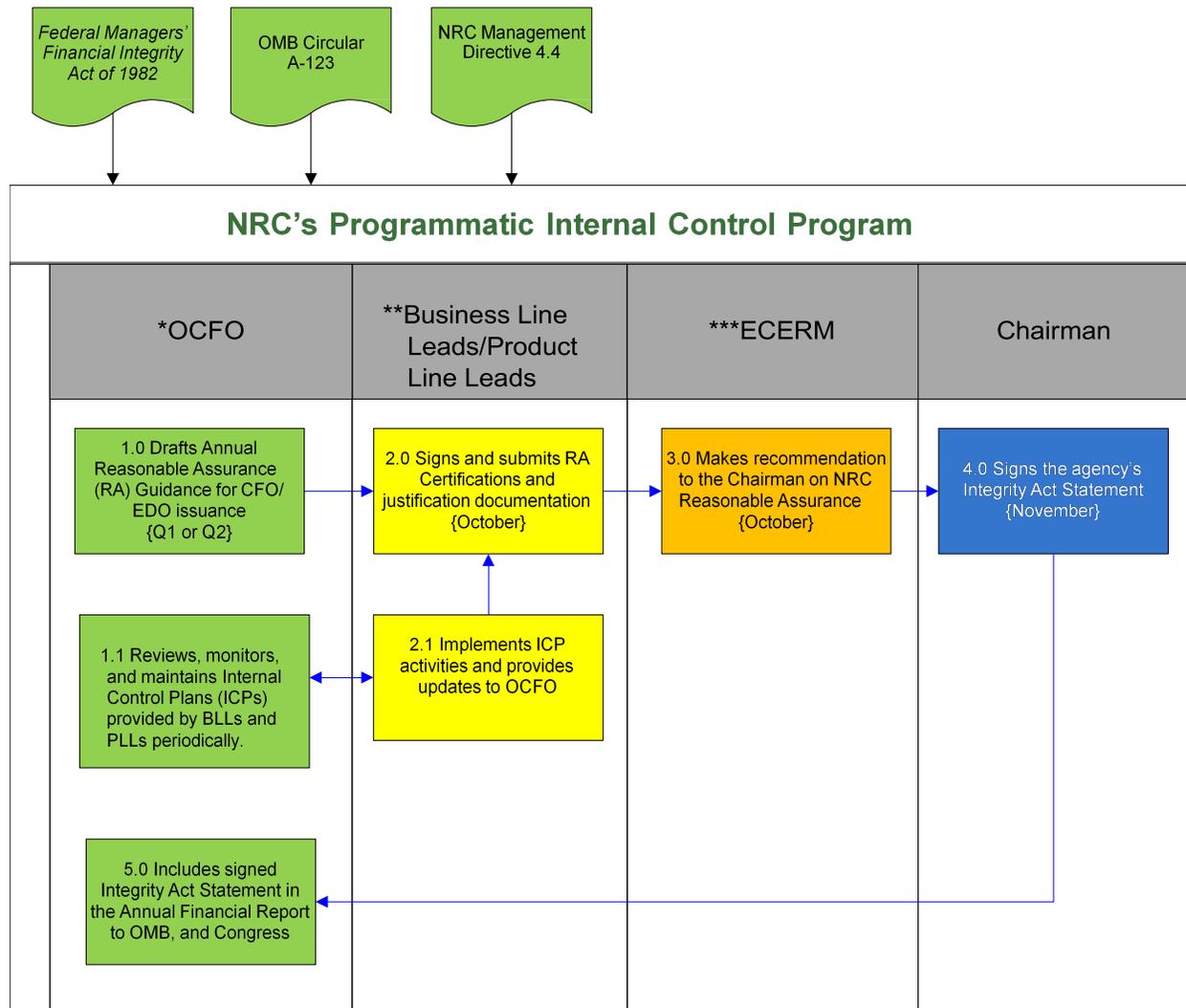


Figure 3. NRC’s Federal Managers’ Financial Integrity Act of 1982 (FMFIA) Governance Framework

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, chaired by the CFO, is responsible for ensuring the agency complies with Appendix A of OMB Circular A-123, “Internal Control over Financial Reporting.” 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 staff coordinates the agency’s reasonable assurance process, serves as liaisons between the CFO and BLLs/Product Line Leads (PLLs), and provides technical expertise, guidance, training, and administration for compliance with FMFIA. For the purpose of this handbook, PLLs are considered business line leads. 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 decisionmaking.



*OCFO administers the Programmatic Internal Control Program and Reasonable Assurance Certification processes and supports the business lines throughout the year

**NRC Business Line and Product Line Lead is the senior executive (office director) of the respective lines.

***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.

Figure 4. NRC Programmatic Internal Control Program

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

1. To help agencies comply with the requirements of the FMFIA, the Government Accountability Office (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, and sets the tone for the organization, which influences desired behaviors and outcomes. Leaders should ask themselves, "What activities should NRC staff perform to meet the agency's mission?" Examples include strategic planning, ethics program, open door policy, and safety culture climate surveys.
 - (b) **Risk Assessment:** identification and analysis of key points of failure to reduce or eliminate the potential for disruptive events. It is the basis for determining how risks should be managed. It is management's responsibility to define risk tolerance and risk mitigation strategies.
 - (c) **Control Activities:** specific policies, procedures, techniques, and mechanisms that help provide reasonable assurance that objectives will be met. Examples include proper segregation of duties, physical controls over assets, rulemakings, and inspections.
 - (d) **Information and Communication:** the process of ensuring the appropriate information is disseminated to the appropriate entities to facilitate timely, effective decisionmaking. Examples include Staff Requirements Memoranda, SECY papers, white papers, Yellow Announcements, and public meetings.
 - (e) **Monitoring:** the process of continuous assessment of control activities, and activities that have internal control implications, to provide reasonable assurance that operation, reporting, and legal/regulatory objectives are met. Examples include the reactor and fuel cycle oversight programs and the agency executive leadership and advisory councils.

C. Internal Control Plan (ICP)

Each NRC BLL will develop the Internal Control Plan (ICP) for their business line. The ICP is a tool used to effectively monitor the business line's internal control program. The ICP should include internal control activities related to programmatic, administrative, and financial operations. The ICP also provides a vehicle for tracking required corrective actions.

D. Training

The course, “Internal Control - A Path Forward to Accountability” (iLearn Course #270147), is designed to demonstrate how the agency complies with the requirements of the Integrity Act, OMB Circular A-123, and GAO’s Green Book. This is awareness training and, as such, demonstrates how current agency activities meet these external requirements and how they are integrated into NRC daily operations. This training was issued as a mandatory, one-time only course for all agency employees and new hires.

IV. NRC INTERNAL CONTROL OVER FINANCIAL REPORTING

Recent government-wide initiatives have also contributed to improvements in financial management and placed greater emphasis on implementing and maintaining effective internal control over financial reporting.

Office of Management and Budget Circular A-123

OMB Circular A-123, Appendix A, “Internal Control over Financial Reporting,” requires Federal agencies to assess the effectiveness of internal control over financial reporting and to prepare a separate annual statement of assurance. The NRC has adopted a rotational testing plan to assess the effectiveness of internal control over financial reporting. Two of the eight key processes (financial reporting and information technology) are significant enough to include each year of the test plan cycle. The remaining six key processes (budget execution, disbursements, payroll, procurement, property, and revenue) are tested once in a 2-year cycle. Reasonable assurance of internal control over financial reporting is based on the results of these evaluations. The Senior Assessment Team (SAT) approves the testing plan annually, and provides strategic oversight and direction for the internal control assessments.

V. REASONABLE ASSURANCE CERTIFICATIONS AND AGENCY STATEMENT OF ASSURANCE

A. Overview

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

The NRC is required to provide a statement of assurance on the effectiveness of internal control over financial reporting as of June 30 of each fiscal year. The NRC also is required to submit an overall statement of assurance as of September 30 of each fiscal year, in accordance with FMFIA requirements. Both statements are combined in the agency's "Statement of Assurance," also referred to as "Integrity Act Statement," signed by the Chairman.

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

1. The BLL/PLL is responsible for signing the business/product line's annual reasonable assurance certification. The annual reasonable assurance certification is based on information from all relevant programmatic internal control activities, and activities that have internal control implications, as well as other sources of information provided by the agency's SAT and independent audit reports.
2. The partner offices are responsible for helping the business line achieve its intended results by conducting its operations in a manner that allows the BLL/PLL to sign the annual Reasonable Assurance Certification under the Integrity Act.

C. Executive Committee on Enterprise Risk Management (ECERM)

At the end of the fiscal year, the ECERM assesses the agency's programmatic operations, financial systems, and internal control over financial reporting. The ECERM reports to the NRC Chairman if there are any internal control deficiencies that are serious enough to require reporting as a weakness or noncompliance, and the ECERM makes a recommendation to the Chairman to sign the agency's Integrity Act Statement.

D. Agency Statement of Assurance (Integrity Act Statement)

The Chairman signs the agency's Integrity Act Statement, which is submitted to OMB and Congress. The Chairman's signature indicates that NRC senior management and staff have evaluated the status of its internal control, financial reporting processes, and

financial systems, pursuant to the Integrity Act and the FFMIA, and either confirms or denies reasonable assurance that the NRC internal control achieves its intended results.

VI. DEFINITIONS

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.

Deficiency or Internal Control Weakness

The breakdown of internal control in a program or administrative activity that does not meet the criteria of a material weakness or reportable condition, but that 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 Chief Financial Officer and co-chaired by the Executive Director for Operations, whose membership includes senior agency managers, that is responsible for assessing, monitoring, and providing oversight and strategic direction for agency programmatic and financial internal control. The predecessor organization to the ECERM was the Executive Committee on Internal Control.

Material Weakness

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

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 the Office of Management and Budget and the Government Accountability Office 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 (by a Business Line Lead)

An annual statement of assurance that summarizes, as of September 30, the business line's compliance with the requirements of the Integrity Act that relates to internal control over programmatic operations and financial reporting. Business Line Leads submit reasonable assurance certifications to the Office of the Chief Financial Officer.

Reportable Condition

A control deficiency or combination of control deficiencies that in management's judgment represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives.

Statement of Assurance (Integrity Act Statement)

An annual statement required by the Integrity Act that represents the Chairman'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 systems of programs, financial reporting, information technology systems, and programmatic controls based upon a fiscal year, October 1 through September 30.