OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Audit of the NRC's Implementation of the Enterprise Risk Management Process

OIG-21-A-16
September 28, 2021

All publicly available OIG reports (including this report) are accessible through the NRC's website at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

September 28, 2021

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

FROM: Eric Rivera ***/RA/***
Acting Assistant Inspector General for Audit

SUBJECT: AUDIT OF THE NRC'S IMPLEMENTATION OF THE ENTERPRISE RISK MANAGEMENT PROCESS (OIG-21-A-16)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of the NRC's Implementation of the Enterprise Risk Management Process*.

The report presents the results of the subject audit. Following the September 2, 2021, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendation(s) within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow-up as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Vicki Foster, Team Leader, at (301) 415-5909.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-21-A-16

September 28, 2021

Results in Brief

Why We Did This Review

The United States (U.S.) Nuclear Regulatory Commission (NRC) established an enterprise risk management (ERM) framework pursuant to the U.S. Office of Management and Budget Circular No. A-123 (OMB Circular A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control*. ERM is an agency-wide approach to address the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risk only within silos. ERM can improve mission delivery, reduce costs, and focus corrective actions towards key risks.

The NRC leveraged its existing Quarterly Performance Review process to document and communicate enterprise risks, which is led by the Office of the Executive Director for Operations (OEDO). The NRC also leveraged its existing reasonable assurance process to report on ERM, which is led by the Office of the Chief Financial Officer (OCFO).

Audit of the NRC's Implementation of the Enterprise Risk Management Process

What We Found

The NRC has implemented an ERM process with a governance framework; however, the effectiveness of the process can improve through better alignment with OMB Circular A-123 and enhanced quality assurance measures over the ERM process.

Specifically, the Office of the Inspector General (OIG) found that the NRC needs a consistent understanding of the agency's risk appetite, needs to have an official risk profile addressing all components, and needs to use a maturity model approach to fully follow federal regulation and good practices. These issues occur because the NRC's risk appetite statement does not exist, agency policy and guidance need improvement, and the NRC stalled its progress on implementing a maturity model approach. Correcting this misalignment with OMB Circular A-123 will enhance the "Be riskSMART" initiative and improve forecasting of agency resources.

The OIG also found that the NRC is deficient in documenting and communicating quality information and ERM-specific training, despite federal regulation and good practices that urge the NRC to do so. This deficiency occurs because quality assurance measures, including OEDO oversight for the ERM process, need strengthening, and ERM-specific training is not sufficient. Properly communicating internal information and prioritizing ERM-specific training will maximize the advantages of ERM.

What We Recommend

This report makes eight recommendations to improve the alignment with OMB Circular A-123 and quality assurance over the ERM process, to include updating policies and procedures, using a maturity model approach, and requiring training.

Agency management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

CFO	Chief Financial Officer
ECERM	Executive Committee on Enterprise Risk Management
EDO	Executive Director for Operations
ERM	Enterprise Risk Management
GAO	Government Accountability Office
GPRAMA	GPRA [Government Performance and Results Act] Modernization Act of 2010
NRC	United States Nuclear Regulatory Commission
OCFO	Office of the Chief Financial Officer
OEDO	Office of the Executive Director for Operations
OIG	Office of the Inspector General
OMB	United States Office of Management and Budget
PSAT	Programmatic Senior Assessment Team
QPR	Quarterly Performance Review

I. BACKGROUND

The United States (U.S.) Nuclear Regulatory Commission (NRC) is mandated by Public Law 111-352, the *GPRA* [Government Performance and Results Act] *Modernization Act of 2010* (GPRAMA) to establish strategic goals and performance plans, report the performance results to the U.S. Congress, and make the performance results available to the public. In addition, Public Law 97-255, the *Federal Managers' Financial Integrity Act of 1982* (Integrity Act) requires the NRC to have ongoing evaluations and reports of the adequacy of internal accounting and administrative controls.

The U.S. Office of Management and Budget Circular No. A-123 (OMB Circular A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control,* requires federal agencies to implement an enterprise risk management (ERM) capability coordinated with the strategic planning and strategic review process established by the GPRAMA, and the internal control processes required by the Integrity Act. Section II of OMB Circular A-123 incorporates the GPRAMA strategic planning and review through ERM, while Section VI captures the reporting of ERM in the Integrity Act reporting on internal controls. Throughout OMB Circular A-123, "…the terms 'Must' and 'Will' denote a requirement that management will comply with in all cases. 'Should,' indicates a presumptively mandatory requirement except in circumstances where the requirement is not relevant for the Agency."

Enterprise Risks

Enterprise risks are risks that could cause losses or jeopardize an agency's ability to carry-out the mission. Risk types include reputational, compliance, financial, legal, legislative, operational, political, reporting, and strategic. An example of an agency enterprise risk is unfilled mission critical positions across the entire organization, which could threaten the accomplishment of the mission.

According to OMB Circular A-123, "ERM is an effective Agency-wide approach to addressing the full spectrum of the organization's external

and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risk only within silos." ERM can improve "…mission delivery, reduce costs, and focus corrective actions towards key risks."

Appendix B of this report provides a table of risk terminology.

ERM at the NRC

To satisfy both the ERM management practices and reporting pursuant to integration of ERM sections of OMB Circular A-123, the NRC's ERM process includes implementation and reporting activities.

The NRC's ERM Implementation Activities

The NRC's ERM implementation activities address the ERM management practices section of OMB Circular A-123; these activities encompass the Quarterly Performance Review (QPR) process, Programmatic Senior Assessment Team (PSAT) review, and Executive Committee on ERM (ECERM) review. The NRC leveraged the agency's existing QPR process to document and communicate enterprise risks. Management Directive 6.9, *Performance Management,* established the QPR process led by the Office of the Executive Director for Operations (OEDO) to collaborate with business lines through quarterly meetings that enable senior managers to "…proactively identify, prioritize, and mitigate areas at risk of impacting the NRC's assets, activities, or operations." In addition, Management Directive 6.9 ensures compliance with the agency performance and reporting requirements of the GPRAMA.

In the context of ERM, the QPR process is a cross-coordination approach to identify and agree on enterprise risks. There are three main groups involved in ERM implementation activities: business lines,[1] the PSAT, and the ECERM. There are NRC leaders that are included in more than one of these groups, resulting in overlapping roles as business lines lead, PSAT member, and/or ECERM member.

[1] In this audit report, references to business lines encompass business lines, product lines, and partner offices, unless otherwise noted.

Directed by OEDO Procedure - 0960, *Enterprise Risk Management Reporting Instructions*, business lines identify and document risks on the QPR Dashboard located on the OEDO Executive Performance Management System SharePoint site. For each risk, business lines enter the risk description, likelihood, impact, mitigation plan, and progress in the QPR Dashboard. Business lines also rate risk likelihoods and impacts as high, medium, or low prior to the QPR meetings. Risks with high impact and medium or high likelihood have a corresponding action in the business lines Internal Control Plan. Business lines track mitigation strategies for addressing risks through ticketed actions, procedures, risk owners, and internal controls.

Risks that are rated with high likelihood and high impact, have agencywide implication, or could be of strategic importance to the agency, are marked as potential PSAT risks and must be discussed during each QPR meeting. Non-PSAT risks may also be discussed during the QPR meetings, as appropriate.

The PSAT[2] is responsible for determining if the risks presented in the QPR meeting by the business lines are significant enough to impact the agency's ability to meet its mission or the strategic goals. The PSAT informs the ECERM of the ERM focus areas by providing a list of agreed-upon PSAT risks. The PSAT risks plot to a heat map[3] based on the assigned and agreed upon risk likelihood and impact ratings. The heat map is discussed at the QPR meetings and the semi-annual ECERM meetings.

Generally, the ECERM[4] consists of senior leadership from the OEDO and the Office of the Chief Financial Officer (OCFO) who meet semi-annually. The ECERM provides strategic oversight for all NRC programs and operations, finalizes ERM focus areas, reviews business lines' reasonable assurance certifications, and makes a recommendation to the Chairman

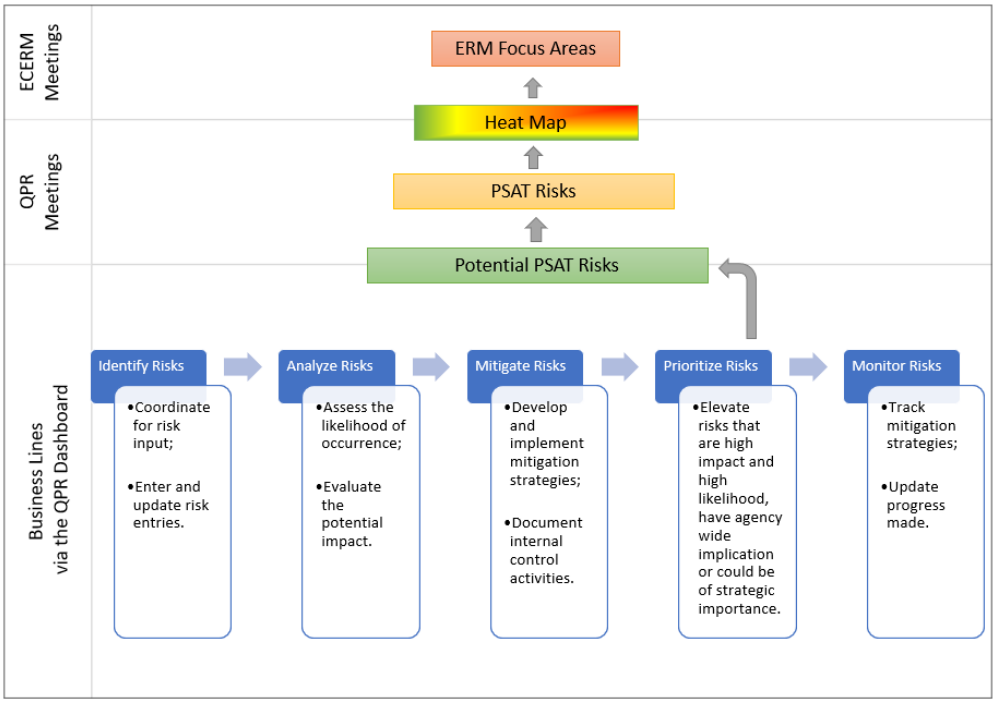
[2] Generally, the PSAT are comprised by a group of office directors. For a detailed listing of the composition of the PSAT, please see Appendix C.

[3] A heat map is a tool used to visually compare multiple risks to decide the top risks and assign a priority to each.

[4] The ECERM is comprised of the Executive Director for Operations (EDO), Chair; the Chief Financial Officer (CFO), Co-Chair; the Deputy EDOs, members; the Assistant for Operations, member; the General Counsel, advisory member; and, the Inspector General, advisory member.

annually on the state of internal control and ERM. Figure 1 illustrates the NRC's ERM implementation activities.

Figure 1: The NRC's ERM Implementation Activities



Source: OIG Generated

The NRC's ERM Reporting Activities

The NRC's ERM reporting activities address the reporting pursuant to integration of the ERM section of OMB Circular A-123, and leverage the agency's existing reasonable assurance process. Management Directive 4.4, *Enterprise Risk Management and Internal Control* stipulates the roles and responsibilities in the ERM process to ensure the agency meets the requirements of OMB Circular A-123 and the Integrity Act. Per Management Directive 4.4, the OCFO coordinates and leads the reasonable assurance process.

Like the NRC's ERM implementation activities, the reasonable assurance process is also a cross-coordination approach to agree on the agency's reporting of reasonable assurance, of which a portion addresses ERM. There are four main groups of responsibility involved in ERM reporting: the business lines, the EDO, the CFO, and the NRC Chairman.

Business lines certify[5] reasonable assurance as directed by the CFO and EDO joint memorandum, *Fiscal Year 2020 Enterprise Risk Management, Programmatic Internal Control and Reasonable Assurance Guidance.* Business lines submit reasonable assurance certifications to the OCFO Internal Control Team, which provides support for the reasonable assurance recommendation to the CFO, and informs a joint memorandum from the CFO and the EDO.

Through the NRC's ERM implementation activities, the ECERM finalizes ERM focus areas, reviews the business lines' assurance certifications, and recommends to the Chairman annually on the state of ERM. Following the second semi-annual ECERM meeting, the CFO and the EDO will jointly issue a memorandum to the Chairman recommending a status on the reporting of reasonable assurance, of which a portion addresses ERM.

Lastly, considering the joint memorandum from the EDO and the CFO, the Chairman signs the agency's Integrity Act statement published annually in the Agency Financial Report, as required by OMB Circular A-123. A portion of this Integrity Act statement focuses on the reasonable assurance of ERM.

[5] Three independent NRC offices outside of the NRC's business lines' structure also certify reasonable assurance: the Atomic Safety and Licensing Board Panel, the Office of Commission Appellate Adjudication, and the Office of Investigations.

II. OBJECTIVE

The audit objective was to assess the effectiveness of the NRC's ERM process. Appendix A of this report contains information on the audit scope and methodology.

III. FINDINGS

The NRC has implemented an ERM process with a governance framework; however, the effectiveness of the process can improve through better alignment with OMB Circular A-123, and enhanced quality assurance measures over the ERM process.

A. The NRC's ERM Process Needs to be Aligned with OMB Circular A-123 Requirements

The NRC needs a consistent understanding of the agency's risk appetite, needs to have an official risk profile addressing all components, and needs to use a maturity model approach, to fully follow federal regulation and good practices. These issues occur because the NRC's risk appetite statement does not exist, agency policy and guidance need improvement, and the NRC stalled its progress on implementing a maturity model approach. Correcting this misalignment with OMB Circular A-123 will enhance the "Be riskSMART"[6] initiative, and improve forecasting of agency resources.

[6] The "Be riskSMART" framework supports the NRC's risk transformation initiative. There are four focus areas the NRC identified to achieve its vision of becoming a more modern risk-informed regulator: "focus on our people," "innovation," "using technology," and "Be riskSMART."

What Is Required

Federal regulation and good practices require an understanding of risk appetite, a risk profile addressing components, and the usage of a maturity model approach.

Understanding of Risk Appetite

OMB Circular A-123 requires that agencies "…must have a solid understanding of their risk appetite…" Additionally, the Government Accountability Office (GAO) report, GAO-17-63, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk,* recommends setting an organizational risk appetite. A risk appetite is the broad-based amount of risk an organization is willing to accept to pursue its mission or vision. The risk appetite is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives. Additionally, the risk appetite should be evaluated regularly and adjusted accordingly to meet the needs of the organization.

Risk Profile Addressing Components and Elements

OMB Circular A-123 states that an agency must maintain a risk profile. A risk profile is the documented and prioritized overall assessment of the range of specific risks the organization faces. The risk profile is a prioritized inventory of the most significant identified risks that have been assessed through the risk assessment process and differs from a risk register, which is an inventory of risks. According to OMB Circular A-123, risk profiles should contain seven components and corresponding elements under each component. Agencies must also have a solid understanding of the risk appetite to create a comprehensive enterprise-level risk profile. The risk profile must consider risks from a portfolio perspective.

Use a Maturity Model Approach for ERM

OMB Circular A-123 and GAO-17-63 direct agencies to develop a maturity model approach to adopting an ERM framework and building an ERM program.

What We Found

The NRC is misaligned from OMB Circular A-123 by not consistently understanding the agency's risk appetite, lacking an official risk profile addressing all components, and not using a maturity model approach.

Agency Managers Need a Consistent Understanding of the NRC's Risk Appetite

Agency managers need a consistent understanding of the NRC's risk appetite. Agency managers across the OEDO, the OCFO, and other offices did not consistently articulate the NRC's risk appetite. This inconsistency in understanding the NRC's risk appetite was evidenced by equating the risk appetite to the risk triplet method, opining that different risk appetites exist for the QPR and the ECERM meetings, inability to articulate the determination of the agency's risk appetite, and not describing a risk appetite.

Lack of Official Risk Profile Addressing All Risk Profile Components and Elements

The NRC lacks an official agency risk profile that addresses all risk profile components and elements. The OEDO and OCFO did not provide the official risk profile in response to a data call requesting it. Furthermore, NRC personnel with ERM responsibilities conveyed various viewpoints about the existence of the risk profile, and identified it as the heat map, the ECERM slide presentation, or through the ECERM meeting discussion, which is not documented by either the OEDO or the OCFO.

Although OMB Circular A-123 clearly distinguishes a risk register from a risk profile, the NRC uses the QPR Dashboard as a risk register for documenting programmatic risks by business lines. Risks in the QPR Dashboard are prioritized and discussed at the QPR meetings and the ECERM meetings. The ECERM members finalize the risk ratings and the list of ERM focus areas. The NRC did not provide a risk profile document with a prioritized inventory of the significant risks that also addresses the components required by OMB Circular A-123. Consequently, the OIG used the QPR Dashboard information to determine whether the NRC met the component and element requirements of a risk profile, per OMB

Circular A-123. The OIG found six out of seven risk profile components do not have elements fully addressed. Appendix D specifies the components the NRC has not addressed.

Maturity Model Approach is Not Used in Implementing ERM

The NRC does not use a maturity model approach for ERM. The OCFO confirmed that the NRC does not currently use a maturity model approach, but acknowledged the benefit of using a maturity model approach in implementing ERM. Specifically, the OCFO stated that using a maturity model approach allows agencies to assess, "what they are doing right and what they can do better."

Why This Occurred

The misalignment with OMB Circular A-123 in the NRC's ERM process occurred because a risk appetite statement does not exist, agency policy and guidance need improvement, and progress stalled on implementing a maturity model approach.

A Risk Appetite Statement Does Not Exist

The first reason for misalignment with OMB Circular A-123 is the absence of a documented risk appetite statement. Agency managers throughout the NRC confirmed there is no documented risk appetite statement. Although a formally documented risk appetite statement is not required by OMB Circular A-123, agency officials conveyed that the agency's risk appetite is not commonly understood across the NRC.

Agency Policy and Guidance Need Improvement

The second reason for misalignment with OMB Circular A-123 is the need to improve agency policy and guidance. For example, Management Directive 4.4 and OEDO Procedure - 0960 are silent on the designation of the NRC's official risk profile.

According to OMB Circular A-123, no less than annually, the Chief Financial Officers Act agencies must prepare a complete risk profile where key findings should be made available for discussion with the OMB as part

of the agency Strategic Review meetings. However, the NRC was granted an exemption from attending the agency Strategic Review meetings with the OMB since 2011. The OMB confirmed to the OIG that the NRC's status as a "…fee-funded, independent agency…" provided the basis for granting the NRC exemption from publishing Agency Priority Goals on Performance.gov; subsequently relieving the NRC from attending the Strategic Review meetings with the OMB. As a result, the risk profile is not a deliverable to the OMB. Despite this exemption, both Management Directive 4.4 and OEDO Procedure - 0960 reference the risk profile as deliverable to the OMB on the risk hierarchy. This exemption from attending the agency Strategic Review meetings may have contributed to the NRC not designating the official risk profile.

OEDO Procedure - 0960 does not require staff to address the following risk profile component elements:

- Explicit identification or reference to strategic, operations, reporting, and compliance objectives;
- Classification of a risk as new or continuous;
- Description and rating of risk likelihood of the inherent risk;
- Formulation of risk responses based on the risk appetite;
- Identification and description of the residual risk;
- Description and rating of risk impact of the residual risk; and,
- Consideration or preclusion of the public reporting of risks.

Lastly, the *Fiscal Year 2020 Enterprise Risk Management, Programmatic Internal Control and Reasonable Assurance Guidance,* Enclosure 1, sets too high, the risk ratings that require internal control actions, based on OMB Circular A-123 requirements. OMB Circular A-123 requires risks with at least medium risk likelihood and medium risk impact ratings to have corresponding internal control activities. However, Enclosure 1 directs business lines to have corresponding internal control activities in the Internal Control Plans for risks rated in the QPR Dashboard with high impact and medium or high likelihood.

Progress Stalled on Using a Maturity Model Approach for ERM

The OEDO and the OCFO collaboratively attempted to assess the maturity level of the NRC's ERM process for application with an agreed upon maturity model approach, but the effort stalled. This maturity model assessment did not progress because the NRC followed a draft maturity model. As a result, the maturity model approach did not advance to receive approval from OEDO management for implementation and use. Alternatively, the NRC personnel with ERM responsibilities could have adopted a maturity model from a document referenced heavily in GAO-17-63. GAO-17-63 references the Chief Financial Officers and Performance Improvement Councils*, Playbook: Enterprise Risk Management for the U.S. Federal Government* (Playbook), issued in July 2016. This Playbook provides three examples of ERM maturity models for agency use.

Why This Is Important

By aligning the NRC ERM efforts with OMB Circular A-123, the agency is better positioned to enhance its "Be riskSMART" initiative and improve forecasting of agency resources.

NUREG/KM-0016, *Be riskSMART: Guidance for Integrating Risk Insights into NRC Decisions* ("Be riskSMART") issued in March 2021, is a framework tool available to staff to assist in risk-based decision making across various sectors in the agency. "Be riskSMART" supports the benefits of a risk appetite, noting that a widely understood risk appetite is essential in aiding decision making about risks. Additionally, a commonly understood risk appetite changes the overall cultural challenge of inconsistent management support and expectations regarding risk. "Be riskSMART" explains, "an organization can establish a risk appetite philosophy," and cites the example of the *U.S. Agency for International Development Risk Appetite Statement – June 2018*. Despite this reference, under the current ERM process, the NRC's risk appetite is not documented or commonly understood by the NRC.

Additionally, ERM necessarily links to strategic planning, which includes allocating agency resource needs in accordance with the risk to the agency's strategic plan. With rapidly evolving threats, information technology is often considered high risk for agencies. If the NRC better

aligns its program with OMB Circular A-123 and GAO-17-63, foreseen information technology issues, could be forecasted as "…areas at risk of impacting the NRC's assets, activities, or operations" through the ERM process, which are the intended outcomes of the QPR meetings, as noted in the fiscal year 2020 QPR meeting agendas.

Recommendations

The OIG recommends that the Executive Director for Operations:

1. Develop and implement a process to periodically communicate a consistently understood agency risk appetite;

2. Revise the agency policies and guidance to:

   a. Designate the official agency risk profile document and remove references to it as a U.S. Office of Management and Budget (OMB) deliverable in Management Directive 4.4, *Enterprise Risk Management and Internal Control* and Office of the Executive Director for Operations Procedure 0960, *Enterprise Risk Management Reporting Instructions*.

   b. Fully address the risk profile components and elements in accordance with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*; and,

3. Implement an enterprise risk management maturity model approach by selecting an appropriate model, assessing current practices per the model, and making progress in advancing the model.

B. Lack of Quality Assurance Over the ERM Process

The NRC is deficient in documenting and communicating quality information and ERM-specific training, despite federal regulation and good practices that urge the NRC to do so. This deficiency occurs because quality assurance measures need strengthening, including the OEDO oversight for the ERM process, and ERM-specific training is not sufficient. Properly communicating internal information and prioritizing ERM-specific training will maximize the advantages of ERM.

What Is Required

Federal regulation and good practices recommend communication and documentation of quality information, and ERM-specific training.

Communication and Documentation of Quality Information

The GAO *Standards for Internal Control in the Federal* Government (GAO Green Book) states that management should communicate and document quality information throughout an agency. Management is required to clearly document significant events in a manner that allows the documentation to be readily available for examination. Quality information is appropriate, current, complete, accurate, accessible, and provided timely.

Training for ERM-Specific Duties

The GAO Green Book states that management should train individuals to have the knowledge, skills, and abilities to carry out assigned responsibilities. "Training is aimed at developing and retaining employee knowledge, skills, and abilities to meet changing organizational needs." Additionally, GAO-17-63 suggests that agencies train employees on the ERM approach.

What We Found

Documentation of Information and Communication Needs Improvement

Documentation of quality information and internal communication needs improvement. Management decision making is not fully documented in the QPR meetings and the ECERM meetings. The QPR meeting summaries and ECERM presentation slides do not document management decision-making of risks such as a status change to non-PSAT risk, risk rating changes, or risk management action changes. Specifically, in fiscal year 2020:

- 12 of 19 potential PSAT risks in the QPR Dashboard were undocumented in the second quarter QPR meeting summary;
- 13 of 19 potential PSAT risks in the QPR Dashboard were undocumented in the third quarter QPR meeting summary;
- 22 of 25 potential PSAT risks in the QPR Dashboard were undocumented in the fourth quarter QPR meeting summary;
- 2 of 19 third quarter potential PSAT risks from the QPR Dashboard were undocumented in the second semi-annual ECERM meeting presentation slides; and,
- 8 of 25 fourth quarter potential PSAT risks from the QPR Dashboard were undocumented in the second semi-annual ECERM meeting presentation slides.

Additionally, the OCFO and the OEDO confirmed there are no ECERM meeting minutes recording the management decisions resulting from the meeting discussions.

The OEDO and the OCFO both use the business lines structure in the NRC's ERM process. However, the OEDO's business lines list for the QPR process that is part of ERM implementation activities does not match the OCFO's business lines list for the reasonable assurance process that is required for ERM reporting activities. Specifically, the OEDO's business lines list on the OEDO's Executive Performance Management System SharePoint site, provided to the OIG through a data call requesting the

fiscal year 2020 business/product lines, did not include the Policy Support Product Line. The OCFO's business lines list from Enclosure 2 of the *Fiscal Year 2020 Enterprise Risk Management, Programmatic Internal Control and Reasonable Assurance Guidance,* did not include the High-Level Waste Business Line.

The NRC has provided varying explanations for deviating from the business lines structure specific to the QPR or reasonable assurance processes. Instances in which the agency are forced to deviate from the business lines structure for either the QPR or reasonable assurance processes should be noted. For example, the OCFO identified one such deviation from the business lines structure in the reasonable assurance process within Enclosure 2 of the *Fiscal Year 2020 Enterprise Risk Management, Programmatic Internal Control and Reasonable Assurance Guidance,* which required three additional offices to certify reasonable assurance.

In addition, risk entries in the QPR Dashboard do not fully follow OEDO Procedure - 0960. Specifically, the QPR Dashboard contained inappropriate, outdated, and missing entries. Inappropriate entries included citing an office in a field requiring identification of an individual, and duplication of risk identification numbers. The outdated entry was the unchanged GAO and OIG audit recommendation risk, despite the release of new audit reports or closure of recommendations, ultimately changing risk to the agency. Finally, risks in the QPR Dashboard were missing entries identifying risk owners, linking risks to strategic planning, likelihood level, mitigation efforts, and performance monitoring.

During fiscal year 2020, the fourth quarter QPR risks were not captured in the Integrity Act statement, effective as of September 30, 2020. The fourth quarter fiscal year 2020 QPR meeting occurred one month after the final ECERM meeting that decides the ECERM focus areas, and recommends the agency's reasonable assurance for the Chairman. According to the NRC, fourth quarter QPR meetings are purposely conducted in such a manner as to allow business lines time to review, input, and finalize risks. As a result, the fourth quarter fiscal year 2020 risks were not captured in that current fiscal year's Integrity Act statement.

ERM-Specific Training is Insufficient

ERM-specific training is insufficient because most NRC personnel with ERM responsibilities have not taken ERM-specific training and the limited ERM training offered by the NRC lacks depth to aid in ERM implementation within agency management practices. Of 19 individuals with ERM responsibilities, including the OEDO, the OCFO, and other office directors, none disclosed having taken an ERM-specific training course during their tenure at the NRC. For example, two individuals in the OEDO admitted that the OCFO previously offered a training course on OMB Circular A-123 called *Internal Control – A Path Forward to Accountability.* However, upon further review, this training did not include ERM-specific concepts such as risk profile, risk profile components and elements, and maturity model. One individual conveyed participation in an interagency rotation at the OMB, which provided in-depth experience regarding the maturity model approach; however, application of the risk profile, components, or elements were not described as part of this experience.

Furthermore, the OIG evaluated 28 training courses in the NRC's Talent Management System that addressed risk, and discovered one recorded webinar, *Are You in Control or Are You at Risk?* which addresses relevant ERM-specific concepts at a high-level, such as risk profile, risk profile components, maturity model approach, ERM linkage to strategic planning, and consideration of the public reporting of risks. This webinar lacks specific information providing step-by-step options on ERM implementation in agency management practices, however, such as the risk profile component elements, different ways a maturity model approach can be implemented, and different approaches to link ERM to strategic planning. Finally, the OEDO personnel with ERM implementation activity responsibilities did not register or complete this ERM recorded webinar during their tasking of ERM responsibilities between fiscal years 2018 through 2020.

Why This Occurred

The quality assurance deficiencies in the ERM process occurred because the OEDO's oversight needs strengthening, and ERM-specific training is not required by the NRC.

The OEDO Oversight of the ERM Process Needs Strengthening

The OEDO's oversight of the implementation of the ERM process through the existing QPR process needs strengthening. The OEDO should ensure that business lines fully perform practices in the QPR process, such that QPR Dashboard entries follow OEDO Procedure - 0960. The OEDO should also ensure that QPR and ECERM meetings fully inform and document management decision-making of risks.

Communication of common information between the OEDO and the OCFO requires improvement. For example, the OEDO and the OCFO should coordinate to have a common business lines structure list, since both are collectively used in the ERM process. Additionally, Management Directive 4.4 and Management Directive 6.9 do not cross reference each other to note the linkage between the QPR and reasonable assurance processes for ERM. Specifically, the following are missing:

- Explanation of the expanded risk responsibilities added to the QPR process in Management Directive 6.9;
- Description of the role and responsibilities of the PSAT in evaluating agency risks in the QPR process in Management Directive 6.9;
- Specification of the ECERM's role in decision-making of agency PSAT risks and ERM focus areas in Management Directive 4.4;
- Connection of Management Directive 4.4 to Management Directive 6.9, clearly showing that ERM implementation activities through the QPR process eventually lead to the ERM focus areas and the reporting of ERM in the Integrity Act statement; and,
- Inclusion of Management Directive 4.4 and OEDO Procedure – 0960 in the "Section VI. References" of Management Directive 6.9.

Finally, OEDO Procedure - 0960 does not clarify the effective dates for the quarterly risks and whether the fourth quarter risks are incorporated in the consideration for the current fiscal year Integrity Act statement. Furthermore, the NRC personnel with ERM responsibilities conveyed different effective dates for the risks in the QPR process, including the fiscal year quarter end dates, due dates for updating the QPR Dashboard each quarter, and the date of the QPR meetings.

The NRC Does Not Require Formal ERM-Specific Training

The NRC does not require formal ERM-specific training. The *Are You in Control or Are You at Risk?* webinar is not mandatory for current NRC personnel with ERM responsibilities in the OEDO, OCFO, and offices throughout the NRC as business lines leads. The former CFO, who led the recorded webinar, indicated that a mandatory ERM-specific training would follow; however, this did not occur.

NRC personnel with ERM responsibilities for the QPR process would benefit from formal training courses that cover ERM-specific concepts, such as risk profile, components and elements in a risk profile, maturity model approach, or linkage of ERM to strategic planning.

Why This Is Important

By adequately communicating internal information and prioritizing ERM-specific training, the agency will maximize the advantages of ERM.

The NRC Could Maximize the Advantages of ERM

Under the current operation of ERM, the NRC is jeopardizing maximization of the advantages of ERM. The NRC's ERM process quality assurance weaknesses have an agencywide impact on transparency and collaboration. OMB Circular A-123 notes: "An open and transparent culture results in the earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient government."

Additionally, by not prioritizing ERM-specific training, NRC personnel with responsibilities in the ERM process may not be as up to date with

developments in ERM. According to GAO-17-63, not prioritizing ERM-specific training may hinder the development of a risk-informed culture to ensure all employees can effectively raise risks.

Recommendations

The OIG recommends that the Executive Director for Operations:

4. Establish and monitor implementation of procedures to ensure that Quarterly Performance Review (QPR) practices are fully performed, such as completion of the QPR Dashboard entries, and recordation of all management decisions of risk in the QPR meeting summaries and Executive Committee on Enterprise Risk Management meeting minutes;

5. Reconcile the business lines structure with the Office of the Chief Financial Officer to have a common business lines structure list. (Deviations from the common business lines structure list for either the Quarterly Performance Review or reasonable assurance processes may be clarified with applicable justification noted);

6. Update policies and guidance to address Management Directive 4.4, *Enterprise Risk Management and Internal Control,* and Management Directive 6.9, *Performance Management,* links to the Quarterly Performance Review (QPR) and reasonable assurance processes to accurately reflect that both agency processes address different aspects of enterprise risk management (ERM). This includes, but is not limited to:

    a. Updating Management Directive 6.9 for the expanded risk responsibilities added to the QPR process;

    b. Explaining the role of the Programmatic Senior Assessment Team (PSAT) in the QPR process in Management Directive 6.9;

    c. Specifying the Executive Committee on ERM (ECERM) role in decision-making of PSAT risks and ECERM focus areas in Management Directive 4.4;

d. Cross-referencing Management Directive 4.4 to Management Directive 6.9 to clearly show that ERM implementation activities through the QPR process eventually lead to the ERM focus areas and the reporting of ERM in the Integrity Act statement; and,

e. Including Management Directive 4.4 and Office of the Executive Director for Operations (OEDO) Procedure - 0960 in Management Directive 6.9, "Section VI. References;"

7. Update policies and guidance to clarify the effective date of the quarterly risks in the Quarterly Performance Review (QPR) process; and,

8. Require enterprise risk management-specific training that addresses U.S. Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* requirements and current best practices, and periodically provide them to NRC personnel with ERM responsibilities.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

The OIG recommends that the Executive Director for Operations:

1. Develop and implement a process to periodically communicate a consistently understood agency risk appetite;

2. Revise agency policies and guidance to:

   a. Designate the official agency risk profile document and remove references to it as a U.S. Office of Management and Budget (OMB) deliverable in Management Directive 4.4, *Enterprise Risk Management and Internal Control* and Office of the Executive Director for Operations Procedure 0960, *Enterprise Risk Management Reporting Instructions*.

   b. Fully address the risk profile components and elements in accordance with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*;

3. Implement an enterprise risk management maturity model approach by selecting an appropriate model, assessing current practices per the model, and making progress in advancing the model;

4. Establish and monitor implementation of procedures to ensure that Quarterly Performance Review (QPR) practices are fully performed, such as completion of the QPR Dashboard entries, and recordation of all management decisions of risk in the QPR meeting summaries and the Executive Committee on Enterprise Risk Management meeting minutes;

5. Reconcile the business lines structure with the Office of the Chief Financial Officer to have a common business lines structure list. (Deviations from the common business lines structure list for either the Quarterly Performance Review or reasonable assurance processes may be clarified with applicable justification noted);

6. Update policies and guidance to address Management Directive 4.4, *Enterprise Risk Management and Internal Control,* and Management Directive 6.9, *Performance Management,* links to the Quarterly Performance Review (QPR) and reasonable assurance processes to accurately reflect that both agency processes address different aspects of enterprise risk management (ERM). This includes, but is not limited to:

    a. Updating Management Directive 6.9 for the expanded risk responsibilities added to the QPR process;

    b. Explaining the role of the Programmatic Senior Assessment Team (PSAT) in the QPR process in Management Directive 6.9;

    c. Specifying the Executive Committee on ERM (ECERM) role in decision-making of PSAT risks and ECERM focus areas in Management Directive 4.4;

    d. Cross-referencing Management Directive 4.4 to Management Directive 6.9 to clearly show that ERM implementation activities through the QPR process eventually lead to the ERM focus areas and the reporting of ERM in the Integrity Act statement; and,

    e. Including Management Directive 4.4 and Office of the Executive Director for Operations (OEDO) Procedure - 0960 in Management Directive 6.9, "Section VI. References;"

7. Update policies and guidance to clarify the effective date of the quarterly risks in the Quarterly Performance Review (QPR) process; and,

8. Require enterprise risk management-specific training that addresses U.S. Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* requirements and current best practices, and periodically provide them to NRC personnel with ERM responsibilities.

V. AGENCY COMMENTS

An exit conference was held with the agency on September 2, 2021. Agency management reviewed and provided comments to the discussion draft version of this report, which the OIG incorporated, as appropriate. Subsequently, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to assess the effectiveness of the NRC's ERM process.

Scope

The audit focused on the NRC's ERM process. Where appropriate, the OIG reviewed the linkages of ERM to the internal control and governance processes. We conducted this performance audit at NRC headquarters (Rockville, Maryland) from February 2021 to July 2021. The audit scope was limited to fiscal year 2020 data and current NRC employees.

Enterprise risks with subsets of additional, specific requirements beyond those required by OMB Circular A-123 or GAO-17-63, such as ERM of information systems, cybersecurity, or privacy risks, were excluded from this audit.

Internal controls related to the audit objective were reviewed and analyzed. Specifically, the OIG reviewed the components of control environment, risk assessment, and information and communication. Within those components, the OIG reviewed the principles of demonstrating commitment to integrity and ethical values; exercising oversight responsibility; establishing structure, responsibility, and authority; defining objectives and risk tolerances; identifying, analyzing, and responding to risk; assessing fraud risk; identifying, analyzing, and responding to change; using quality information; and, communicating internally and externally.

Methodology

Throughout this audit, the OIG reviewed relevant criteria and guidance. The OIG's document review included:

- The Federal Managers' Financial Integrity Act;

- The GPRA [Government Performance and Results Act] Modernization Act of 2010;
- Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*;
- Government Accountability Office report, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk* (GAO-17-63);
- Management Directive 4.4, *Enterprise Risk Management and Internal Control;*
- Management Directive 6.9, *Performance Management;*
- Office of the Executive Director for Operations (OEDO) Procedure - 0960, *Enterprise Risk Management Reporting Instructions;* and,
- Executive Director for Operations (EDO)/Chief Financial Officer (CFO) Memorandum, *Fiscal Year 2020 Enterprise Risk Management, Programmatic Internal Control and Reasonable Assurance Guidance* dated December 16, 2019.

The OIG also interviewed current year NRC personnel that have ERM responsibilities. The OIG interviewed the ECERM members, business lines leads, and program managers of ERM at the NRC. These interviews included the EDO, the CFO, the Chief Information Officer, office directors, division directors, and key staff responsible for the NRC's ERM program. The OIG also received an OEDO demonstration of the QPR Dashboard to observe how risk owners input risks. The OIG's analysis included comparing data from the QPR Dashboard and OMB Circular A-123 requirements.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Throughout the audit, auditors considered the possibility of fraud, waste, and abuse in the program.

The audit was conducted by Vicki Foster, Team Leader; Tincy Thomas de Colón, Audit Manager; Angel Wang, Senior Auditor; and Karen Corado, Management Analyst.

Appendix B

RISK TERMINOLOGY

Term	Definition
A. Enterprise Risk	Risks that could cause losses or jeopardize an agency's ability to carry-out the mission.
B. Enterprise Risk Types:	
1. Compliance Risk	Risk of failing to comply with applicable laws and regulations and the risk of failing to detect and report activities that are not compliant with statutory, regulatory, or organizational requirements.
2. Financial Risk	Risk that could result in a negative impact to the agency (waste or loss of funds/assets).
3. Legal Risk	Risk associated with legal or regulatory actions and the agency capacity to consummate important transactions, enforce contractual agreements, or meet compliance and ethical requirements.
4. Legislative Risk	Risk that legislation could significantly alter the mission (funding, customer base, level of resources, services, and products) of the agency.
5. Operational Risk	Risk of direct or indirect loss or other negative effects to an agency due to inadequate or failed internal processes arising from people, systems, or from external events that impair those internal processes, people, or systems.
6. Political Risk	Risk that may arise due to actions taken by Congress, the Executive Branch, or other key policy makers that could potentially impact business operations, the achievement of the agency's strategic and tactical objectives, or existing statutory and regulatory authorities.
7. Reporting Risk	The risk associated with the accuracy and timeliness of information needed within the organization to support decision making and performance evaluation, as well as outside the organization to meet standards, regulations, and stakeholder expectations.
8. Reputational Risk	Risk that a failure to manage risk, external events, and external media or to fail to fulfill the agency's role (whether such failure is actual or perceived) could diminish the stature, credibility, or effectiveness of the agency.
9. Strategic Risk	Risk that would prevent an area from accomplishing its objectives including meeting the mission.
C. Enterprise Risk Management (ERM)	An effective agency-wide approach to addressing the full spectrum of the organization's significant internal and external risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos.

Term	Definition
D. ERM Maturity Model Approach	An organization matures as it progresses from having no structure or doing *ad hoc* work to an optimized or leadership structure. A more mature risk organization will not only react to issues that arise but will be able to articulate the risks it faces and have in place management strategies to respond to those risks. It will look forward and try to predict what could happen and develop strategies to meet those contingencies. It will have risk dialogue within and across silos.
E. Inherent Risk	The exposure arising from a specific risk before any action has been taken to manage it beyond normal operations.
F. Residual Risk	The exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent risk assessment.
G. Risk Appetite	The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives.
H. Risk Impact	The effect or impact of a risk occurring.
1. High Risk Impact	The impact could preclude or highly impair the agency's ability to achieve one or more of its objectives or performance goals.
2. Medium Risk Impact	The impact could significantly affect the agency's ability to achieve one or more of its objectives or performance goals.
3. Low Risk Impact	The impact will not significantly affect the agency's ability to achieve one or more of its objectives or performance goals.
I. Risk Likelihood	The probability or likelihood of a risk occurring.
1. High Risk Likelihood	The risk is very likely or reasonably expected to occur.
2. Medium Risk Likelihood	The risk is more likely to occur than unlikely.
3. Low Risk Likelihood	The risk is unlikely to occur.
J. Risk Profile	The documented and prioritized overall assessment of the range of specific risks faced by the organization. OMB Circular A-123 requires seven risk profile components and several corresponding elements to be addressed when documenting the risk profile.
K. Risk Register	A complete inventory of risks.
L. Risk Tolerance	The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

Appendix C

Programmatic Senior Assessment Team (PSAT)

Title	PSAT Role	Business/Product Line
Executive Director for Operations (EDO)	Chair	Not applicable
Chief Financial Officer (CFO)	Co-Chair	Financial Management Product Line Policy Support Product Line
Office Director, Office of Nuclear Reactor Regulation	Member	Operating Reactors Business Line New Reactors Business Line
Office Director, Office of Nuclear Materials Safety and Safeguards	Member	Fuel Facilities Business Line Spent Fuel Storage and Transportation Business Line Nuclear Materials Users Business Line Decommissioning and Low-Level Waste Business Line High Level Waste Business Line
Office Director, Office of Small Business and Civil Rights	Member	Outreach Product Line
Chief Information Officer	Member	Information Technology/Information Management Resources Product Line
Chief Human Capital Officer	Member	Human Resources Management Product Line Training Product Line
Office Director, Office of Administration	Member	Administrative Services Product Line Acquisition Product Line
Performance Improvement Officer/Assistant for Operations, Office of the Executive Director for Operations	Member	Not applicable

Appendix D

RISK PROFILE COMPONENTS NOT FULLY ADDRESSED

OMB Circular A-123 Risk Profile Component	Elements of Risk Profile Component Not Fully Addressed	Reason for Deficiency
Objectives	Strategic, operations, reporting, and compliance objectives	The applicable strategic, operations, reporting, and compliance objectives are not explicitly identified, listed, or referenced in the QPR Dashboard.
Risk Identification	New or continuous risk	Identification of whether a risk is new or continuous is not specifically notated in the QPR Dashboard.
	Inherent and residual risk	Residual risk is not specifically identified and described in the QPR Dashboard.
Inherent Risk Assessment	Risk likelihood/impact ratings of high, medium, or low before risk management	Risk likelihood level and descriptions are not instructed to be assessed before risk management in the QPR Dashboard.
Current Risk Response	Formulation of risk responses based on risk appetite and risk tolerance levels	The NRC does not have a formally documented risk appetite statement. Accordingly, risk responses in the QPR Dashboard are not based on a risk appetite.
	Internal control activities for at least medium likelihood and medium impact risks	Thresholds requiring internal control activities for ERM risks are too high. As a result, this element is not met.
	Internal control activities for risks that can be publicly reported	The QPR Dashboard does not address the consideration or preclusion of the public reporting of risks.
Residual Risk Assessment	High, medium, or low risk likelihood and impact ratings after risk management	The QPR Dashboard does not address risk impact description and rating after risk management.
Proposed Action	Formulation of risk responses after risk management are based on risk appetite and risk tolerance levels	The same Current Risk Response component elements apply to the Proposed Action component after risk management, therefore these elements are not met.
	Internal control activities for at least medium likelihood and medium impact risks after risk management	
	Internal control activities for risks that can be publicly reported after risk management	

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TTY/TDD: 7-1-1, or 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email the OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.