



## **MEMORANDUM**

**DATE:** August 27, 2024

**TO:** Mirela Gavrilas  
Executive Director for Operations

**FROM:** Hruta Virkar, CPA /*RA*/  
Assistant Inspector General for Audits & Evaluations

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

**REFERENCE:** ACTING ASSOCIATE DIRECTOR FOR OPERATIONS  
MEMORANDUM DATED JUNE 28, 2024

Attached is the Office of the Inspector General's (OIG) analysis and status of recommendation as discussed in the agency's response dated June 28, 2024. Based on this response, recommendation 5 is now closed. Recommendations 1 through 4 and 6 through 8 remain open and resolved. Please provide an updated status of the open, resolved recommendations by January 31, 2025.

If you have any questions or concerns, please call me at 301.415.1982 or Paul Rades, Team Leader, at 301.415.6228.

Attachment:  
As stated

cc: J. Martin, Acting ADO  
M. Meyer, DADO  
S. Miotla, DADO  
J. Jolicoeur, OEDO  
OIG Liaison Resource  
EDO ACS Distribution

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

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

Agency Response  
Dated June 28, 2024: The Office of the Executive Director for Operations (OEDO) staff is working to develop the agency's risk appetite statement. Upon completion, the staff will implement a process to periodically communicate a consistently understood agency risk appetite. The agency's risk appetite statement and associated process for periodic communication will be incorporated in the next revision to OEDO Procedure 0960.

Target Completion Date: September 30, 2024

OIG Analysis: The proposed actions meet the recommendation's intent. The OIG will close this recommendation after reviewing the risk appetite statement and verifying that the revised OEDO Procedure 0960, *Enterprise Risk Management Reporting Instructions*, specifies the agency's determination, implementation, and communication frequency regarding its risk appetite.

**Status:** Open: Resolved.

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

- Recommendation 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*.

Agency Response  
Dated June 28, 2024:

The staff is revising agency policy and guidance to designate the official agency risk profile document, remove references of OMB deliverables, and fully address risk profile components and elements in accordance with OMB Circular A-123. The staff completed the revision to Management Directive 4.4 on April 3, 2023 ([ML23073A073](#)). The staff will revise OEDO Procedure 0960 as proposed in this recommendation.

Target Completion Date: September 30, 2024

OIG Analysis: The proposed actions meet the recommendation's intent. The OIG reviewed the revised Management Directive 4.4 and confirmed that references to the agency risk profile as an OMB deliverable was removed.

The OIG will close this recommendation after reviewing the revised OEDO Procedure 0960, *Enterprise Risk Management Reporting Instructions*, clarifying the designation of the official agency risk profile document, and detailing the risk profile components and elements in accordance with OMB Circular A-123.

**Status:** Open: Resolved.

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

Recommendation 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.

Agency Response

Dated June 28, 2024:

The revised Playbook: Enterprise Risk Management for the U.S. Federal Government guidance was issued by OMB in November 2022 and included an unchanged Federal ERM Maturity Model, previously assessed in June 2020. Staff will conduct a follow-up assessment using the Federal ERM Maturity Model and continue making progress with the implementation of this maturity model, including the development of an action plan with milestones to assess current practices and further advance the model.

Target Completion Date: September 30, 2024

OIG Analysis:

The proposed actions meet the recommendation's intent. The OIG will close this recommendation after verifying the NRC's adoption and implementation of an appropriate enterprise risk management maturity model by selecting an appropriate model, assessing current practices per the model, and making progress in advancing the model through the milestones in the maturity model action plan.

**Status:**

Open: Resolved.

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

Recommendation 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.

Agency Response

Dated June 28, 2024:

The staff plans to update OEDO Procedure 0960 with best practices based on this recommendation, including, but not limited to completion of QPR Dashboard entries, and recordation of all management decisions of risk in the QPR meeting summaries and the Executive Committee on ERM (ECERM) meeting minutes. The NRC staff has continued implementing this recommendation by ensuring that management decisions of risk discussed during the QPR meetings and ECERM meetings are recorded in the meeting minutes.

Target Completion Date: September 30, 2024

OIG Analysis:

The proposed actions meet the recommendation's intent. The OIG will close this recommendation when it reviews the revisions to the OEDO Procedure 0960, *Enterprise Risk Management Reporting Instructions*, and verifies the inclusion of procedures to ensure that QPR practices are fully performed, such as comprehensively completed QPR Dashboard entries and all risk-related management decisions resulting from QPR and ECERM meetings are recorded in the meeting summaries.

**Status:**

Open: Resolved.

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

Recommendation 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).

Agency Response  
Dated June 28, 2024:

The OEDO and the OCFO staff worked together to establish and maintain a common business lines structure list. ERM, Internal Control, and Reasonable Assurance guidance was issued on February 6, 2024 ([ML24018A217](#)). Enclosure 2 of the guidance provides the business line structure list and identifies the lead and partner offices. OEDO restructured the Quarterly Performance Review meeting starting with the May 7, 2024, FY 2024 Quarter 2 meeting to present the Programmatic Senior Assessment Team risks in order of severity using the heat map in the Strategic Planning Application. The [meeting agenda](#) and [summary](#) described the change in process. Any future deviations from this business line structure for reasonable assurance or using risk severity for QPR discussions will be identified with written justification in the resulting product.

Target Completion Date: Completed

OIG Analysis: The OIG reviewed the ERM, Internal Control, and Reasonable Assurance guidance issued on February 6, 2024, and the meeting agenda and summary provided by the NRC. These documents show that the business lines list has been reconciled and implemented. Therefore, this recommendation is now closed.

**Status:** Closed.

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

- Recommendation 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."

Agency Response  
Dated June 28, 2024:

The NRC staff is revising the guidance documents as mentioned in this recommendation. The staff completed the revision to Management Directive 4.4 on April 3, 2023 ([ML23073A073](#)). The annual reassurance guidance document was issued on February 6, 2024 ([ML24018A217](#)). The revised Management Directive 6.9 is to be issued in September 2024.

Target Completion Date: September 30, 2024

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

Recommendation 6 (continued):

OIG Analysis:                   The proposed actions meet the recommendation's intent. The OIG previously closed 6.c. The OIG will close this recommendation after review of the revised Management Directive 6.9 for recommendations 6.a, 6.b, 6.d, and 6.e.

**Status:**                        Open: Resolved.



**Audit Report**  
**AUDIT OF THE NRC’s IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

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

Agency Response

Dated June 28, 2024:

The OEDO is working with OCFO to update policies and guidance to clarify the effective date of the quarterly risks in the QPR process. The staff completed the revision to Management Directive 4.4 on April 3, 2023 ([ML23073A073](#)) to state that: “At the end of the fiscal year, including the results of the fourth quarter of the fiscal year to address OIG Audit OIG-21-A-16, recommendation 7, the ECERM assesses the agency’s programmatic operations, financial systems, and internal control over reporting.” Instructions for inclusion of fourth-quarter risks will also be included in the revision to OEDO Procedure 0960.

Target Completion Date: September 30, 2024

OIG Analysis:

The proposed actions meet the recommendation’s intent. The OIG reviewed the revised Management Directive 4.4 and confirmed that the agency clarified that fourth-quarter risks are to be included in the QPR process.

The OIG will close this recommendation after verifying the agency’s revision to OEDO Procedure 0960, which includes instructions for including fourth-quarter risks.

**Status:**

Open: Resolved.

**Audit Report**  
**AUDIT OF THE NRC's IMPLEMENTATION OF THE ENTERPRISE**  
**RISK MANAGEMENT PROCESS**  
**Status of Recommendations**  
**(OIG-21-A-16)**

Recommendation 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.

Agency Response

Dated June 28, 2024:

The staff is developing ERM training that will address OMB Circular A-123 requirements and best practices. This training will periodically be provided to staff with ERM responsibilities. Additional time to complete this item is necessary to incorporate changes to guidance documents into the training materials and to facilitate further staff collaboration within the NRC to finalize the training.

Target Completion Date: December 31, 2024

OIG Analysis:

The proposed actions meet the recommendation's intent. The OIG will close this recommendation after verifying (1) the ERM training addresses OMB Circular A-123 requirements and current best practices, and (2) the revised policies pertaining to ERM specify the competencies required for the NRC personnel with ERM responsibilities and the ERM training requirement frequency.

**Status:**

Open: Resolved.