U.S. AbilityOne Commission
Office of Inspector General

Audit Report:
The AbilityOne Commission's ERM Program is Not Fully Effective

OA-2024-01

December 20, 2024

U.S. AbilityOne Commission
Office of Inspector General

355 E Street SW (OIG Suite 335)
Washington, DC 20024-3243

December 20, 2024

MEMORANDUM

TO: Jeffrey A. Koses
Chairperson
U.S. AbilityOne Commission

Kimberly M. Zeich
Executive Director
U.S. AbilityOne Commission

FROM: Stefania Pozzi Porter
Inspector General
U.S. AbilityOne Commission OIG

Report issued thru:
Lauretta A. L. Joseph
Acting Assistant Inspector General for Audit
U.S. AbilityOne Commission OIG

SUBJECT: Final Audit Report of the U.S. AbilityOne Commission's Enterprise Risk Management (ERM) program

We are pleased to transmit the following **final** audit report on the U.S. AbilityOne Commission's enterprise risk management (ERM) program. The U.S. AbilityOne Commission Office of Inspector General (OIG), Office of Audit conducted the audit and issued this report.

We appreciate the Commission's assistance during the course of the audit. If you have any questions, please contact me or Lauretta A. L. Joseph, Assistant IG for Evaluation and acting Assistant IG for Audit at 571-329-3419 or at ljoseph@oig.abilityone.gov.

cc: Chai Feldblum
Vice Chairperson
U.S. AbilityOne Commission

Kelvin Wood
Chief of Staff
U.S. AbilityOne Commission

Results in Brief

Audit The AbilityOne Commission's ERM Program is Not Fully Effective

Office of Inspector General Report No. OA-2024-01. Report Date: December 20, 2024

Why We Performed This Audit

The OIG Audit office initiated this audit based upon an assessment of program risks. Our audit objective was to determine whether the U.S. AbilityOne Commission's (Commission) enterprise risk management (ERM) process is effective and used to make risk-based decisions.

What We Audited

To answer our audit objective, we 1) reviewed laws, regulations, policies, and procedures applicable to the ERM program implementation, 2) conducted interviews with key personnel, and 3) analyzed data, reports, and other supporting documentation related to ERM. The audit period covered the Commission's ERM program from October 1, 2021, through September 30, 2023. The audit was performed in accordance with the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards.

What We Found

Although the Commission has designed and implemented a formal ERM program, the OIG determined that the ERM program is not fully effective. This could impact the Commission's ability to make fully informed risk-based decisions. Specifically, we found that the Commission's ERM process and related internal controls need improvements, and the Commission lacked the ERM training to identify and correct these improvement areas.

What We Recommend

The OIG recommended that the Commission ensure that the appropriate individuals are trained through a structured ERM program training, assess and update existing ERM policies and procedures, and research and adopt an appropriate ERM maturity model. We also recommended that the Commission develop and implement effective key controls and results assessment, include a process in the ERM program to document management's determination of key process decisions for its other process considerations, and develop and implement a process for tracking the consolidation of risks.

Table of Contents

Objectives and Background

Objective

Our audit objective was to determine if the Commission's ERM process is effective and used to make risk-based decisions.

Background

Commission – Including Central Nonprofit Agency (CNA) and Nonprofit Agency (NPA) Structure

Enacted in 1938, the Wagner-O'Day Act established the Committee on Purchases of Blind-Made Products to provide employment opportunities for the blind. In 1971, Congress amended and expanded the Wagner-O'Day Act with the Javits-Wagner-O'Day (JWOD) Act[1] to include persons with significant disabilities. The 1971 amendments also changed the name of the Committee to the Committee for Purchase from People Who Are Blind or Severely Disabled to reflect the expanded capabilities of the JWOD Program. The program is currently a source of employment for approximately 37,000 people who are blind or have significant disabilities and are employed by approximately 420 NPAs nationwide.

In 2006, the JWOD Program was renamed the AbilityOne Program, and the Committee took on the branded name of the U.S. AbilityOne Commission (hereinafter referred to as the Commission) in 2011. The Commission is composed of fifteen Presidential appointees: eleven members representing Federal agencies and four members serving as private citizens from the blind and disabled community, bringing their expertise in the field of employment of people who are blind or have significant disabilities. As of September 2024, the Commission has approximately 34 full-time employees who administer and oversee the AbilityOne Program (hereinafter referred to as the Program), which includes over $4 billion in products and services provided to the Federal government annually.

The Commission maintains and publishes a Procurement List (PL) of specific products and services, which Federal agency purchase agents must buy to help meet the department's mission needs. Under the JWOD Act and its implementing Federal regulations codified in title 41 of the U.S. Code of Federal Regulations, chapter 51, the Commission is responsible for establishing the rules, regulations, and policies of the Program. The NPAs[2] furnish the products and services (including military resale commodities) on the PL to the Federal Government.

The Commission delegates certain program management responsibilities to its designated Central Nonprofit Agencies (CNAs). Each NPA is affiliated with a CNA. The CNAs evaluate

[1] United States Code (U.S.C) Title 41, Subtitle IV, Chapter 85, Sections 8501 - 8506
[2] See 41 U.S.C. § 46 et seq., 41 CFR 51-1.3, and 41 CFR 51-2.8(a).

and recommend NPA initial qualification to the Commission and provide regulatory assistance to the NPAs it represents, to facilitate and support the NPAs in maintaining qualification.[3] CNAs recommend which NPA(s) to assign to a particular project, which, if determined to be feasible, becomes a proposed PL addition. The CNAs include:

- National Industries for the Blind (NIB), whose mission is to enhance the personal and economic independence of people who are blind, primarily through creating, sustaining, and improving employment. As of September 30, 2023, NIB had 178 employees and annual revenue of nearly $35 million.

SourceAmerica®, whose mission is to increase the employment of people with disabilities by building strong partnerships with the Federal government and engaging a national network of NPAs and experts. As of September 30, 2023, SA had 478 employees and annual revenue of more than $197 million.

U.S. AbilityOne Commission Office of Inspector General

In 2013, GAO issued a report titled Employing People with Blindness or Severe Disabilities: Enhanced Oversight of the AbilityOne Program Needed. This report stated that the AbilityOne Commission does not have procedures to monitor alleged CNA control violations, nor is there an inspector general to provide independent audit and investigation capabilities for the program, including the CNAs. As a result, GAO presented Congress a consideration of establish an inspector general and provided additional recommendations to the Commission to enhance program oversight.

On December 18, 2015, the Consolidated Appropriations Act of 2016 (P.L. 114-113) amended the Inspector General Act of 1978 (IG Act) and created the Office of Inspector General (OIG) at AbilityOne as a designated federal entity IG. The OIG is responsible for conducting audits, evaluations, and investigations, recommending policies and procedures that promote economy, efficiency, and effectiveness of agency resources and programs, and detecting and preventing fraud, waste, abuse, and mismanagement. The IG Act requires the IG to keep the Commission and Congress fully and currently informed about problems and deficiencies in the Commission's operations and the need for any corrective action.

Enterprise Risk Management

The Office of Management and Budget Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (OMB A-123)[4] underscored the importance of coordinating ERM activities with the strategic planning and review process and internal controls required by the Federal Managers' Financial Integrity Act (FMFIA) and the U.S. Government

[3] See 41 CFR 51-1.3, 51-2.2, 51-3.2, 51-4.2 and 51-4.3.
[4] Office of Management and Budget, Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, amended July 15, 2016, under M-16-17

Accountability Office (GAO)'s Standards for Internal Control in the Federal Government (Green Book).[5]

ERM encompasses the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to identify, assess, and manage risks. It emphasizes the need to integrate and coordinate internal control assessments in support of mission delivery and streamlines internal control reporting by eliminating areas of overlap and duplication. Management uses ERM as a tool that can help leaders anticipate and manage risks possibly affecting the achievement of an agency's objectives as well as consider how multiple risks, when examined as a whole, can present even greater challenges and opportunities.

The OMB A-123

> *requires agencies to integrate risk management and internal control functions. The Circular also establishes an assessment process based on [the Green Book] that management must implement in order to properly assess and improve internal controls over operations, reporting, and compliance.*

Additionally, OMB A-123, section I, explained that

> *[ERM] and Internal Control are components of a governance framework. ERM as a discipline deals with identifying, assessing, and managing risks. Through adequate risk management, agencies can concentrate efforts towards key points of failure and reduce or eliminate the potential for disruptive events…. ERM is viewed as a part of the overall governance process, and internal controls as an integral part of risk management and ERM.*

The OMB A-123 uses the terms "must" and "will" for its requirements and uses "should" as required unless it not relevant for the agency. The Green Book, September 2014, also uses "should" for the required components and principles.

The Green Book, September 2014, "provides managers criteria for designing, implementing, and operating an effective internal control system." The Green Book separated content between required components and principles and the associated guidance contained within attributes. The Green Book "provides managers criteria for designing, implementing, and operating an effective internal control system."

Additionally, the Green Book section OV1.01 explained that

> *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... These objectives and related risks can be broadly classified into one or more of the following three categories: Operations… Reporting… Compliance.*

[5] U.S. Government Accountability Office report number GAO-14-704G, Standards for Internal Control in the Federal Government, September 2014

The Commission developed its ERM program framework and processes in its *Enterprise Risk Management Program Guide* (ERM Guide), dated July 2021. The ERM program was formally established through Commission's internal Policy 51.703, *Enterprise Risk Management Program* that was effective November 29, 2021 (ERM Policy).

Scope and Methodology

The audit covered the period October 1, 2021, through September 30, 2023. We completed our work from November 1, 2023, through October 2024. We conducted the audit in accordance with generally accepted government auditing standards.[6] 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 objective(s). We believe that the evidence obtained provides a reasonable basis for our conclusions based on our objective.

To accomplish our objective, we reviewed laws, regulations, policies, and procedures applicable to the implementation of ERM. This specifically included the OMB A-123, OMB A-11, Green Book, and the Commission's ERM Policy and Guide.[7] Additionally, we conducted interviews with key Commission personnel and analyzed data, reports, and other supporting documentation related to ERM.

We compared the Commission's ERM risk register, which also acts as its risk profile, against the Commission's ERM email communications, meeting notes, and PowerPoint presentations. We reviewed 100 percent of the data provided and determined it was sufficiently reliable for our purposes. Specifically, we reviewed the Commission's

- Enterprise Risk Management Program 101, dated May 17, 2021, and related notes,
- ERM risk register dated April 12, 2023,[8]
- ERM subcommittee meeting emails and related attachments,
- ERM requests for staff input and related meeting details,
- List of ERM meetings for fiscal years 2022 to 2023,
- ERM mitigation planning PowerPoint documents for FY 2021 and 2022,
- ERM Risk Register for FY21-22 Mapped to Draft Strategic Plan, and

[6] U.S. Government Accountability Office report number GAO-21-368G, Government Auditing Standards, April 2021 (also known the Yellow Book).
[7] The audit did not fully evaluate the Commission's ERM Policy and Guide to ensure they were consistent and compliant with federal requirements since we were able to answer our objective without this additional extensive analysis.
[8] This was the latest ERM risk register within our audit period.

- Results of internal controls tested for management review controls (MRC).

The draft report was provided to Commission management for technical comments and management's response on November 8, 2024, and the Commission's Executive Director provided management's response on November 25, 2024. The Commission did not have technical comments to the draft report. See Appendix A for the Commission's management response.

Results

The Commission has designed and implemented a formal ERM program; however, the OIG audit revealed that the ERM program is not fully effective, which could impact the Commission's ability to make informed risk-based decisions. Specifically, the OIG audit identified five components for an effective ERM program were missing from the Commission's current ERM program and identified three areas in which ERM internal controls need improvement.

Also, the audit revealed that due to a lack of appropriate ERM training, the Commission staff lacked the skillset to identify and correct program deficiencies. The audit revealed that the current Commission staff lacked appropriate knowledge of federal ERM program requirements as well as its program design, which has resulted in no detailed internal controls related to ERM.

The above findings are of concern to the OIG because without an effective ERM program, there is an increased likelihood that the Commission will not properly identify, assess, and respond to significant entity-level risks. The OIG has included in this report a list of recommendations to address the issues found.

ERM Program and Process Needs Improvement

The Commission has established an ERM program; however, it is missing five components of an effective ERM program. The following list, numbered 1 through 5, provides information on each of the components missing from the Commission's ERM program.

1. Annual Analyses of Risks Faced to Achieve Strategic Objectives Not Completed

Agencies are required to identify and analyze risks in relation to their strategic objectives. Specifically, OMB A-123, section II part B1, states, "Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan" (See OMB Circular No. A-11, Section 230). Section II also explains that "While agencies cannot respond to all risks related to achieving strategic objectives and performance goals, they must identify, measure, and assess risks related to mission delivery."

Furthermore, OMB A-123, Figure 3, provides ERM development deadlines, specifically stating that all agencies must prepare a complete risk profile no less than annually.

The Commission's risk register was designed to identify correlations between the risk and the strategic objectives.

During the OIG audit, the team conducted a review of the Commission's risk register and profile along with the related meetings notes. The review of these items did not support

that an annual analysis was conducted as required by OMB A-123. The documentation provided by the Commission only demonstrated that once a risk surfaced it was assessed to determine what strategic objectives it could impact.

2. Risk Appetite and Tolerance Levels Not Considered

In responding to current risks OMB A-123, section II part B4, required "Formulation of risk responses should consider the organization's risk appetite and tolerance levels. The development of risk responses should be used to inform decision-making…"

Additionally, OMB A-123, section II part A, stated,

> *Regardless of the governance structure developed, agency governance should include a process for considering risk appetite and tolerance levels. The concept of "risk appetite" is key to achieving effective ERM and is essential to consider in determining risk responses. Although a formally documented risk appetite statement is not required, agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise-level risk profile.*

During the OIG audit, the team conducted a review of the Commission's risk register and related meeting notes. The review of these documents revealed no evidence that the Commission had created a process to consider risk appetite and tolerance levels when assessing risks as required by OMB A-123, section II part B4.

3. Root-Cause Analyses Not Performed

As part of the corrective action plan requirements OMB A-123, section V part B, requires that

> *Agencies should perform a root-cause analysis of the deficiency to ensure that subsequent strategies and plans address the root of the problem and not just the symptoms. Identifying and developing an understanding of the root cause of control deficiencies is management's responsibility.*

The OIG audit revealed that the Root-Cause Analyses was identified within the ERM Policy and Guide as a responsibility of the Risk Analysis Integrated Project Teams (IPT). However, during the OIG audit, the OIG found no evidence that the IPT was operational during the audit period or that root-cause analyses were performed for risks as required by OMB A-123, section V part B.

4. Continual Assessment of Risks Not Conducted

OMB A-123, section II part C, provided the requirements for risk monitoring, stating that

> *The management of risk must be regularly reviewed to monitor whether or not the risk profile has changed and to gain assurance that risk management is effective or if further action is necessary... In addition, the overall risk management process must be subjected to regular review to deliver assurance that it remains appropriate and effective. At a minimum, management's risk management review processes must:*
>
> - *ensure that all aspects of the risk management process are reviewed at least once a year;*
> - *ensure that risks themselves are subjected to review with appropriate frequency; and*
> - *make provisions for alerting the appropriate level of management to new or emerging risks, as well as changes in already identified risks, so that the change can be appropriately addressed.*

The OIG audit revealed that although the Commission developed processes within its ERM Guide, it did not continually monitor and evaluate activities related to its implemented mitigation plan results as required by OMB A-123, section II part C.

Furthermore, there was no evidence of continuous assessment of newly implemented strategies to determine whether the strategies resulted in unintended consequences from internal and external environments.

5. ERM Maturity Model Not Adopted

In accordance with OMB A-123 requirements, the Commission was to "develop a maturity model approach to the adoption of an ERM framework." During the audit review the OIG team was unable to locate an adopted ERM maturity model in the documentation provided by the Commission as required by OMB A-123.

The OIG interviewed the Commission management. During interviews, Commission management confirmed that an ERM maturity model had not been adopted. Additionally, a review of the Commission's ERM Policy and Guide did not indicate that there was an internal policy or procedure related to the adoption and use of an ERM maturity model approach.

Internal Controls Over the ERM Program Need Improvements

The Commission has established internal controls over the ERM program; however, improvements are needed to ensure that the (1) controls are effective, (2) business processes are fully supported, and (3) key decisions are documented. The list numbered 1 through 3 below provides additional information on the ERM program areas that need improvement.

1. Entity-Level Controls Were Ineffective

Section 6.01 of the Green Book states that "Management should define objectives clearly to enable the identification of risks and define risk tolerances." When the OIG conducted its audit, the Commission's identification of risks and defined tolerances was not apparent. The documentation provided by the Commission was not sufficient to support its entity-level control assessment and results assessment.

After a discussion with the Commission regarding this matter, Commission management provided additional documentation for the entity-level control results of key identified business processes. However, the documentation provided was still insufficient to comply with the Green Book standards. For example, there were no identifiable key controls for compliance[9] and operations[10] to mitigate risks to an acceptable level.

The Commission's lack of key controls could ultimately impact the operations effectiveness of the Commission's ERM program, as well as its internal control system. Additionally, the absence of these key controls could (1) diminish the Commission's ability to establish a baseline to properly evaluate its internal controls and (2) prevent the Commission from operating effectively.

2. Business Processes Related to ERM Were Not Fully Supported

Under Principle 10, section 10.01, the Green Book requires that "management should design control activities to achieve objectives and respond to risks." Additionally, section 3.OV3.06. states,

> *In evaluating operating effectiveness, management determines if controls were applied at relevant times during the period under evaluation, the consistency with which they were applied, and by whom or by what means they were applied. If*

[9] Compliance controls assist an entity with meeting the requirements of significant provisions of applicable laws and regulations.
[10] Operations controls assist an entity with ensuring the accomplishment of management's desired performance for planning, productivity, quality, economy, efficiency, or effectiveness of the entity's operations.

> *substantially different controls were used at different times during the period under evaluation, management evaluates operating effectiveness separately for each unique control system.*

During the audit, OIG found that the control the Commission provided to the audit team did not comply with section 10.01 of the Green Book. Specifically, the audit team was unable to use the ERM process information provided by the Commission to recreate the ERM process outlined in the Commission's ERM flowchart. The audit team found that the process information provided was missing key process-supporting documentation. Therefore, the OIG determined that business processes related to ERM were not fully supported and, as a result, could increase the number of variations within the application of the program steps.

3. Better Documentation for Key Decisions Needed

A robust documentation system is the backbone that allows organizations to systematically manage their procedures and processes. Under section OV.4.08, the Green Book emphasizes the importance of documentation stating that

> *Documentation is a necessary part of an effective internal control system. The level and nature of documentation vary based on the size of the entity and the complexity of the operational processes the entity performs. Management uses judgment in determining the extent of documentation that is needed. Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system.*

Strong internal control systems rely on supporting documentation to detail the basis for decisions. The OIG audit revealed that the Commission did not consistently record or maintain key discussions and decisions regarding its ERM process as required by Green Book section OV.4.08. In addition, the Commission did not have a primary documentation method, nor did it specify the need to include supporting documentation in its ERM process for these decisions.

Timely, accurate, and reliable information is also an integral part of internal control operations that can help mitigate risks. Therefore, the quality of information generated or used by management from both internal and external sources is critical to support the function of the Commission's internal controls. To ensure the accuracy, completeness, and reliability of the ERM information provided by the Commission, the OIG performed a documentation review and comparison of two data sets related to the total number of risks in the Commission risk profile. During the documentation review, the OIG identified a discrepancy related to the total number of risks between the two data sets.

When asked about the discrepancy, the Commission stated that the documentation for obsolete and inactive risks was maintained in a different file.

Due to the OIG's finding, the Commission updated its risk register and incorporated a new tab labeled, "Inactive" to consider actions related to inactive risks. Although a step in the right direction, this update to the risk register was completed outside of the audit review period.

The Commission lacked supporting documentation demonstrating the sequence of important actions, rationale, and agreement by pertinent management official decision for key ERM program business decisions. As a result, the Commission could not support the key business decisions that were used to determine the actions that were included, combined, or excluded in its ERM program, since the knowledge generated as part of its decision-making process was not documented. Because the Commission did not have a method to document these key decisions, it is difficult to properly assess the appropriateness and reliability of the key business decisions in relation to the Commission's ERM process.

Lack of ERM Training

In general, the OIG determined that the Commission has not obtained, nor developed, sufficient ERM training to build staff expertise in operating an effective ERM program and related assessment of its internal controls system. The lack of training has contributed to the Commission missing several components of an effective ERM program. Additionally, the Commission's full implementation of its ERM program may be hindered by the lack of understanding of how a fully effective ERM program operates.

1. Commission Staff Lacked Training to Build ERM Expertise

Based on the deficiencies noted in this audit report and conversations with Commission management, the Commission lacked a sufficient understanding of the ERM requirements and the related implementation. While training is not specifically called out as a requirement for the successful implementation and management of an ERM program and process, OMB A-123, section II, discusses the steps of establishing ERM in management practices. OMB A-123 section II specifies that "[t]o complete this circle of risk management the Agencies must incorporate risk awareness into the agencies' culture and ways of doing business." OMB A-123, section I, also states, "Federal leaders and managers… are also responsible for implementing management practices that effectively identify, assess, respond to, and report on risks." Additionally, OMB A-123 requires staff to identify objectives, assess related risks, document internal controls, develop risk mitigation plans, conduct appropriate tests of the operating effectiveness of controls,

report on the results of these tests, and appropriately document the assessment procedures.

The OIG determined that the Commission had offered only one ERM program training since 2021, which consisted of one PowerPoint presentation and lacked sufficient instructions on how to perform relevant ERM activities. Specifically, the 2021 training presentation lacked:

- Instructions on how to identify different types of risks, explain the difference between a component risk, and the risk composition,
- Coverage of OMB A-123's ERM framework elements in detail or how they are interrelated,
- Adequate communication of basic definitions and concepts included in OMB A-123 and the Green Book, and
- Instructions on how to interpret, respond to, and control deficiencies.

The Commission management stated that because there was no staff turnover in positions involved with ERM decision-making, there was no need for additional or continuous training after the 2021 internal ERM training. Additionally, the Commission relies on the use of its existing 2021 ERM Policy and Guide. However, the Commission acknowledged that its ERM policies need to be updated and do not fully represent its current ERM processes.

Conclusions

The Commission's ERM program (1) was missing some elements of an effective ERM program and (2) needs improvements to ensure that controls are in place and effective. Additionally, the Commission's staff lacked adequate training to obtain a sufficient understanding of ERM requirements. The Commission's ERM program progress is hindered by the staff's lack of understanding of how a fully effective ERM program operates. Without an effective ERM program, there is an increased risk that the Commission will not properly identify, assess, and respond to significant entity-level risks. The ineffectiveness of the ERM program could impact the Commission's ability to make informed and accurate risk-based decisions.

Recommendations

The OIG recommends that the AbilityOne Commission

1. Ensure the appropriate individuals are trained through a structured ERM program training to increase knowledge and understanding throughout the organization and share key takeaways and materials with employees at all levels to effectively contribute to the organization's program success.

2. Assess and update the Commission's existing policies and procedures to ensure compliance with federal requirements and that the policies and procedures reflect the processes that it wants to adopt.

3. Research and adopt an appropriate ERM maturity model.

We also recommend that the Commission Chairperson require the CFO to

4. Develop and implement effective key controls that identify risks and assign the Commission's risk tolerances by aligning each control objective with the appropriate control activity and completing an updated entity-level control and results assessment.

5. Include a process in the ERM program to include documenting management's determination of key process decisions for its other process considerations.

6. Develop and implement a process for tracking the consolidation of risks.

Management's Response and Our Evaluation

The Commission's Executive Director acknowledged the results of the report and concurred with the OIG's recommendations. After OIG review and analysis of the responses provided by the Commission, we believe the Commission's proposed corrective actions to be responsive to the recommendations. Specifically,

- The Commission agreed with Recommendation 1 and proposed corrective action, to be completed by September 20, 2025, that meets the intent of the recommendation.
- The Commission agreed with Recommendations 2 and 3 and proposed corrective actions, to be completed by December 31, 2025, that meet the intent of the recommendations.
- The Commission agreed with Recommendation 4 and proposed corrective action, to be completed by April 30, 2026, that meets the intent of the recommendation.
- The Commission agreed with Recommendations 5 and 6 and proposed corrective actions, to be completed by December 31, 2025, that meet the intent of the recommendations.

Appendix

Appendix A - Management Comments

U.S. ABILITYONE COMMISSION
355 E STREET SW, SUITE 325
WASHINGTON, DC 20024

November 25, 2024

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: Kimberly M. Zeich, Executive Director

SUBJECT: Management Comments (Enterprise Risk Management Audit)

We have reviewed the draft audit report of November 8 20, 2024, in which your audit team found that, overall, the U.S. AbilityOne Commission has designed and implemented a formal Enterprise Risk Management (ERM) program. We appreciate the Office of Inspector General's commitment of time and resources to this audit.

The report also found that the ERM program is not fully effective and made recommendations. The Commission concurred with the recommendations. As described in the attached management response, we have developed implementation timelines accordingly.

KIMBERLY ZEICH
Digitally signed by KIMBERLY ZEICH
Date: 2024.11.25 18:54:24 -05'00'

Kimberly M. Zeich
Executive Director
U.S. AbilityOne Commission

Attachment:
Management Response

U.S. ABILITYONE COMMISSION
355 E STREET SW, SUITE 325
WASHINGTON, DC 20024

Finding 1: ERM Program and Process Needs Improvement—
The Commission has established an ERM program; however, it is missing five components of an effective ERM program:

1. **Annual analyses of risks faced to achieve strategic objectives not completed**
2. **Risk appetite and tolerance levels not considered**
3. **Root-cause analyses not performed**
4. **Continual assessment of risks not conducted**
5. **ERM maturity model not adopted**

Recommendations:

1. Assess and update the Commission's existing policies and procedures to ensure compliance with federal requirements and that the policies and procedures reflect the processes that it wants to adopt.

2. Research and adopt an appropriate ERM maturity model.

Management Response:

The Commission concurs with the recommendations. ERM policies and procedures will be reviewed and updated accordingly. The Commission will utilize feedback from the OIG's upcoming assessment of its ERM maturity level in adopting a maturity model. Implementation of recommendations will occur by December 31, 2025.

Finding 2: Internal Controls Over the ERM Program Need Improvements—
The Commission has established internal controls over the ERM program; however, improvements are needed to ensure that the (1) controls are effective, (2) business processes are fully supported, and (3) key decisions are documented.

Recommendations:

1. Develop and implement effective key controls that identify risks and assign the Commission's risk tolerances by aligning each control objective with the appropriate control activity and completing an updated entity-level control and results assessment.

2. Include a process in the ERM program to include documenting management's determination of key process decisions for its other process considerations.

3. Develop and implement a process for tracking the consolidation of risks.

Management Response:

The Commission concurs with the recommendations. For Recommendation 1, the Commission will review its entity-level controls related to risk identification and assess those controls accordingly; implementation will occur by April 30, 2026.

U.S. ABILITYONE COMMISSION
355 E STREET SW, SUITE 325
WASHINGTON, DC 20024

Since the audit commenced in November 2023, the Commission has implemented a standard process for documenting management decisions that occur through its quarterly ERM battle rhythm. For Recommendations 2 and 3, the process will be more formally documented in the Commission's ERM policy; implementation will occur by December 31, 2025.

Finding 3: Lack of ERM Training—
In general, the OIG determined that the Commission has not obtained, nor developed, sufficient ERM training to build staff expertise in operating an effective ERM program and related assessment of its internal controls system. The lack of training has contributed to the Commission missing several components of an effective ERM program

Recommendation:

Ensure the appropriate individuals are trained through a structured ERM program training to increase knowledge and understanding throughout the organization and share key takeaways and materials with employees at all levels to effectively contribute to the organization's program success.

Management Response:

The Commission concurs with the recommendation and will establish ERM training for agency leadership and risk owners. Implementation will occur by September 30, 2025.