U.S. AbilityOne Commission
Office of Inspector General

Assessment of the U.S. AbilityOne Commission's ERM Program Maturity Level

OA-2025-01

March 11, 2025

U.S. AbilityOne Commission
Office of Inspector General

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

March 11, 2025

MEMORANDUM

TO: Robert D. Hogue
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

SUBJECT: Final Report of OIG's Assessment of the U.S. AbilityOne Commission's ERM Program Maturity Level

We are pleased to provide the following **final** evaluation report on the U.S. AbilityOne Commission's enterprise risk management (ERM) program maturity level. The U.S. AbilityOne Commission Office of Inspector General, (OIG) Office of Audit completed this review.

We appreciate the Commission's assistance during the course of the review. 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: Christina Brant
Vice Chairperson
U.S. AbilityOne Commission

Kelvin Wood
Chief of Staff
U.S. AbilityOne Commission

Results in Brief

Evaluation: Assessment of the U.S. AbilityOne Commission's ERM Program Maturity Level

Office of Inspector General Report No. OA-2025-01. Report Date: March 11, 2025

Why We Performed This Evaluation:

The Office of Inspector General (OIG) initiated this review based upon an assessment of program risks. Our objective was to review the U.S. AbilityOne Commission's (Commission) enterprise risk management (ERM) program to assess its maturity level, which will provide the Commission with an overall understanding as to where its current ERM program stands.

What We Evaluated

To answer our review objective, we 1) reviewed laws, regulations, policies, and procedures applicable to the ERM implementation, 2) conducted interviews with key personnel, 3) surveyed Commission leadership and staff to gain their perspectives of the Commission's ERM program for a more comprehensive view of the ERM program maturity, and 4) analyzed data, reports, and other supporting documentation related to ERM. We conducted this review in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of Inspectors General on Integrity and Efficiency.

What We Found

There are five levels in the model we used to assess the Commission's ERM program. The OIG assessment determined that the Commission's ERM program maturity is between level 2, emerging, and level 3, integrated. By conducting its own internal maturity assessment, it can periodically identify gaps in its ERM program and develop plans to mature the program, as necessary.

What We Recommend

The OIG has no specific recommendations associated with this report.

Table of Contents

Objectives and Background 1

Scope and Methodology 5

Results 6

Conclusions 8

Appendix 9

Appendix A Maturity Assessment Ratings 9

Appendix B Management Comments 14

Objectives and Background

Objective

Our objective was to review the Commission's ERM program to assess its maturity level, which will provide an overall understanding as to where the Commission's current ERM program stands.

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 across all fifty states and U.S. territories.

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 nearly $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.

[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).

The Commission delegates certain program management responsibilities to its designated Central Nonprofit Agencies (CNAs). Each NPA is affiliated with a CNA. The CNAs evaluate 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 about 178 employees and annual revenue of about $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 about 478 employees and annual revenue of about $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 asked Congress to consider establishing 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

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.

[3] See 41 CFR 51-1.3, 51-2.2, 51-3.2, 51-4.2 and 51-4.3.

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 Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Enterprise Risk Management (OMB A-123)*[4] recognizes that Federal agencies have diverse missions and are at different levels of maturity in terms of their capacity to fully implement ERM. The Circular states that agencies should develop a maturity model approach to the adoption of an ERM framework and that an agency's approach for developing risk profiles and implementing ERM should be refined and improved each year. This guidance recognizes that not all components of an ERM process may be operational in the initial years, and agency leadership must set priorities for implementation. The Playbook*: Enterprise Risk Management for the Federal Government (Playbook)*[5] provides ERM guidance including a maturity model approach. The Playbook also includes examples of maturity models. The Playbook states

> These models may be used to continually self-assess the maturity of a federal ERM program and its supporting framework. The intent of the models are to provide criteria which can help an organization move forward over time, ultimately embedding ERM practices into daily business operations and strategic decision-making…. These maturity models depict the evolution and maturation of a federal ERM program…. It is also very important to understand that the maturity level does not always move forward.

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 the Commission's internal Policy 51.703*, Enterprise Risk Management Program* that was effective November 29, 2021 (ERM Policy). In our previous audit of the Commission's ERM program, audit report OA-2024-01, we concluded that the Commission had not adopted an ERM maturity model approach.[6] The Commission is currently updating its ERM Policy, and per discussions with the Commission, a maturity model approach had not been adopted at the time of this report.

Our review a Playbook ERM maturity model, which we adapted for use in this maturity level review assessment. Figure 1 shows the simplified ERM maturity model used for the review. A detailed version, including our assessment scores, can be found in Appendix A of this report.

Figure 1. OIG Selected ERM Maturity Model for Review

[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

[5] From the Chief Financial Officers Council and Performance Improvement Council, Playbook: Enterprise Risk Management for the Federal Government, Fall, 2022 update.

[6] AbilityOne OIG, report number OA-2024-01, The AbilityOne Commission's ERM Program is Not Fully Effective, dated December 20, 2024

Level 1 Ad-hoc

- Lacks formal ERM process; initial activities are defined; risk response is reactive; no perceived program benefit; ad hoc discussions at the executive level

Level 2 Emerging

- ERM roles and responsibilities defined; informal governance exists; some risks measured and managed; risk responses are developing; low perceived value to the mission; fragmented executive engagement

Level 3 Integrated

- Formal governance; coordinated ERM program and practices; facilitates knowledge sharing and opportunities for informed risk taking; enterprise risks are routinely measured and managed; risk responses are tactical; moderate perceived value to mission; routine risk discussions at the executive level

Level 4 Institutionalized

- Embedded ERM governance exists; advanced program that facilitates knowledge sharing and opportunities for informed risk taking; majority of enterprise risks are measured quantitatively and qualitatively; risk response is strategic; high perceived value to mission; managed and active risk discussions at the executive level that consider multiple facets of agency operations

Level 5 Optimized

- Effective ERM governance exists; ERM program fully facilitates knowledge sharing and leverages opportunities for informed risk taking; enterprise risks are fully measured and managed; risk response is proactive; transformational value to mission; integrated risk discussions that embeds risk sensing into strategic planning, resource allocation, and decision-making based on risk reward and trade-off issues

Scope and Methodology

The evaluation covered the period October 1, 2021, through September 30, 2024. We completed our work from October 2024, through February 2025. We conducted this assessment in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of Inspectors General on Integrity and Efficiency.

We 1) reviewed laws, regulations, policies, and procedures applicable to the ERM program, 2) conducted interviews with key personnel, 3) surveyed Commission leadership and staff to gain their perspectives of the Commission's ERM program for a more comprehensive view of the ERM program maturity, and 4) analyzed data, reports, and other supporting documentation related to ERM. We also relied on data and information obtained and validated during our audit of the Commission's ERM Program, OIG audit report number OA-2024-01.[7]

Specifically, we reviewed the following applicable criteria related to the ERM program

- OMB Circular A-123,
- The Commission's ERM Guide, July 2021,
- The Commission's ERM Policy, November 29, 2021, and
- ERM Playbook, Fall, 2022 update.

The ERM program maturity assessment was conducted using a rating matrix adapted from the ERM Playbook. The rating matrix had 5 levels of maturity ranging from level 1, ad-hoc to level 5, optimized, see Appendix A.

[7] Audit of the U.S. AbilityOne Commission's Enterprise Risk Management (ERM) program | AbilityOne Office of Inspector General OIG

Results

The Commission's ERM program was established in 2021, and many aspects are still being implemented. Our review assessed the Commission's current ERM maturity level. We analyzed the Commission's ERM maturity using a model that had 5 levels of maturity ranging from level 1, ad-hoc to level 5, optimized. Our assessment indicated that the Commission's ERM program maturity was between level 2, emerging, and level 3, integrated. An internal maturity review would provide opportunities for the Commission to assess the existing gaps in its ERM program and develop plans to mature the program, as necessary.

Commission's ERM Program Maturity is Between Emerging and Integrated

The Commission's average maturity level score was between level 2, emerging, and level 3, integrated. There were five scored domains (1) program attributes, (2) key practices, (3) risk culture, (4) organization benefits, and (5) executive engagement.

1. Program Attributes

The Playbook described the ERM maturity model program attributes domain as "Specific to the key factors an internal ERM program should have when benchmarking itself. This attribute contained expectations for behaviors of individuals who are engaged in the ERM program." Within this domain, we assessed the Commission's ERM program governance, ERM roles and responsibilities, facilitation of knowledge sharing, and ERM framework and processes used for monitoring and reviewing for improvements. We determined that for the program attributes domain, the Commission scored between level 2, emerging, and level 3, integrated, see Appendix A, number 1.

2. Key Practices

In the Playbook, the key practices domain is characterized as "Practices expected to be in place across the organization in terms of how ERM is implemented." Within this domain, we assessed the Commission's ERM program and practices, discipline, monitoring and reporting, measurement and reporting, and risk appetite and tolerances. We determined that for the key practices domain, the Commission scored between level 2, emerging, and level 3, integrated, see Appendix A, number 2.

3. Risk Culture

According to the Playbook the risk culture domain is characterized as the "progression of maturity achieved; how much of a focus is risk within the organization and how embedded is it within the agency's culture; and includes approach to risk response [*sic*]." Within this domain, we evaluated the Commission's risk response and the workforce's understanding of ERM and risk concepts. We determined that for the risk culture domain, the Commission scored between level 2, emerging, and level 3, integrated, see Appendix A, number 3.

4. Organization Benefits

In the Playbook, the organization benefits domain is defined as "The value provided by ERM to the enterprise." Within this domain, we assessed the Commission's perceived value to the mission, perceived benefits, and change adaptability. We determined that for the organization benefits domain, the Commission scored level 2, emerging, see Appendix A, number 4.

5. Executive Engagement

The Playbook described the executive engagement domain as "Tone at the top. Level of overall support." Within this domain, we assessed the ERM program executive engagement, risk discussion and dialog, and executive understanding of ERM and risk awareness. We determined that for the executive engagement domain, the Commission scored between level 3, integrated, and level 4, institutionalized, see Appendix A, number 5.

The Commission's ERM Policy and ERM Guide were established in 2021. Based on the OIG report number OA-2024-01, multiple parts of its ERM program still need to be implemented. We attribute the gaps identified in the previous audit, which included lack of training and incomplete policies and procedures, for a maturity model approach not being adopted. As of January 2025, Commission staff had informed the OIG that the ERM Policy 51.703 was being updated at the time of this report, in response to OIG report number OA-2024-01.

An internal maturity review, based on an adopted maturity model approach, would provide opportunities for the Commission to assess the existing gaps in its ERM program and develop plans to mature the program, as necessary. According to the Playbook, "Federal ERM maturity self-assessments should be a means for agencies to identify next steps in their ERM program maturity curve."

Conclusions

The Commission's ERM program maturity rating between level 2 and 3 provides opportunities for the Commission to improve its ERM program. By conducting its own internal maturity assessment, it can periodically identify gaps in its ERM program and develop plans to mature the program, as necessary.

Management's Response and Our Evaluation

The Commission concurred with the OIG report. The Commission also stated that it plans to use this report to address relevant open recommendations from report OA-2024-01.[8]

[8] Audit of the U.S. AbilityOne Commission's Enterprise Risk Management (ERM) program | AbilityOne Office of Inspector General OIG.

Appendix

Appendix A Maturity Assessment Ratings

		Level 1: Ad-hoc	Level 2: Emerging	Level 3: Integrated	Level 4: Institutionalized	Level 5: Optimized	Maturity Level
1. Program Attributes	1.1	No formal ERM governance exists	Informal ERM governance exists	Formal ERM governance exists	Embedded ERM governance exists	Effective ERM governance exists	2
	1.2	No centralized risk management roles/ responsibilities	Some centralization of ERM responsibilities built into existing roles or siloed in various components	Generally centralized ERM roles/ responsibilities	Centralized and institutionalized ERM roles and responsibilities	Fully centralized ERM roles and responsibilities with CRO reporting directly to the top executive	3
	1.3	ERM program does not facilitate knowledge sharing or leverage opportunities for informed risk taking	ERM program facilitates some knowledge sharing and opportunities for informed risk taking	ERM program generally facilitates knowledge sharing and opportunities for informed risk taking	Advanced ERM program that facilitates knowledge sharing and opportunities for informed risk taking	ERM program fully facilitates knowledge sharing and leverages opportunities for informed risk taking	3
	1.4	Ineffective ERM framework and processes exist	Developing ERM framework and processes	Standardized ERM framework and processes exist with periodic monitoring for framework improvements	Managed ERM framework and processes exist and are regularly monitored and reviewed for improvements	Optimal ERM framework and processes exist and are proactively monitored and reviewed to prepare for the future	2
	Average score for Program Attributes						**2.50**

		Level 1: Ad-hoc	Level 2: Emerging	Level 3: Integrated	Level 4: Institutionalized	Level 5: Optimized	Maturity Level
2. Key Practices	2.1	Ad hoc ERM	Early stages of ERM	Coordinated ERM program and practices	Instilled ERM program and practices integrated with internal tools and data	Predictive ERM program which leverages external data sources that enhance insight and internal/ external horizon scanning to identify emerging risks	3
	2.2	Initial activities defined	Emerging ERM discipline	Defined ERM processes yet not fully integrated	Instilled ERM discipline	Optimal ERM discipline, recognized as best in class	3
	2.3	Reactive monitoring and reporting exists	Informal monitoring and reporting exists	Formal monitoring and reporting exist to support risk prioritization	Embedded monitoring and reporting exist and considers forward-looking/ emerging risk areas to support risk prioritization and decision-making	Effective and efficient monitoring and reporting exist to support forward-looking risk taking, aligned with risk appetite, strategy and budget	1
	2.4	No enterprise risks are measured or managed	Some enterprise risks are measured and managed	Enterprise risks are routinely measured/ managed, primarily qualitatively	Majority of enterprise risks are measured quantitatively and qualitatively, with interdependencies identified and effectively managed	Enterprise risks are fully measured and managed (e.g., through risk modeling/ scenarios)	3

		Level 1: Ad-hoc	Level 2: Emerging	Level 3: Integrated	Level 4: Institutionalized	Level 5: Optimized	Maturity Level
	2.5	No risk appetite in place	Fragmented risk appetite in place	Defined risk appetite in place	Institutionalized risk appetite and tolerances in place	Optimal risk appetite and tolerances established, clearly understood with alerts in place when thresholds exceeded	1
	Average score for Key Practices						**2.20**
3. Risk Culture	3.1	Risk responses are reactive	Risk responses are developing	Risk responses are tactical, supported by action plans implemented in response to high priority risks, and focused on prevention	Risk response is strategic	Risk response is proactive	3
	3.2	Workforce has no understanding of ERM and risk concepts	Workforce has some understanding of ERM and risk concepts	Workforce generally understands ERM and risk concepts	Workforce understands ERM and risk concepts and is encouraged to discuss risk in an open and inclusive environment	Workforce fully understands and embraces ERM, and risk concepts and believes that risk management is everyone's job. There is an open environment that fosters objective discussions about risk across the enterprise	2
	Average score for Risk Culture						**2.50**

		Level 1: Ad-hoc	Level 2: Emerging	Level 3: Integrated	Level 4: Institutionalized	Level 5: Optimized	Maturity Level
4. Organization Benefits	4.1	Unaware of ERM value to mission	Low perceived value to mission	Moderate perceived value to the mission	High perceived value to mission such as preventing issues and creating value	Transformational value to mission	2
	4.2	No perceived benefit	Some benefit, compliance driven	Generally beneficial, informs priorities for risk-based decision-making	Consistently informed risk taking aligned with enterprise strategy (e.g., by identifying and documenting enterprise identifying and documenting enterprise risk/ rewards trade off)	Fully beneficial; proactively informs risk taking, as well as; provides platform for enterprise agility and innovation	2
	4.3	Backward-looking and does not respond to opportunity and change	Slow to adapt to change	Readily adapts to change	Agile and resilient; adaptable to change	Anticipates change; forward-looking	2
	Average score for Organization Benefits						**2.00**
5. Executive Engagement	5.1	Negligible executive engagement	Fragmented executive engagement	Formal executive engagement	High executive engagement	Optimal executive engagement	4
	5.2	Ad-hoc risk discussions/ dialogue at the executive level	Some routine risk discussions/ dialogue at the executive level	Routine risk discussions/ dialogue at the executive level	Managed and active risk discussions/ dialogue at the executive level that consider strategic planning, resource allocation, and decision-making based on risk reward and trade-off issues	Integrated risk discussions/ dialogue that embeds risk sensing into strategic planning, resource allocation, and decision-making based on risk reward and trade-off issues	3

		Level 1: Ad-hoc	Level 2: Emerging	Level 3: Integrated	Level 4: Institutionalized	Level 5: Optimized	Maturity Level
	5.3	No understanding of ERM and minimal risk awareness	Emerging understanding of ERM and risk awareness	General understanding and awareness of ERM and risks, initial training in ERM	Advanced understanding and awareness of ERM and risk; executive ownership at enterprise level	Optimal understanding and awareness of ERM and risk	3
		Average score for Executive Engagement					**3.33**
						Total average maturity level score	**2.51**

Appendix B Management Comments

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

February 19, 2025

MEMORANDUM FOR THE INSPECTOR GENERAL

FROM: Kimberly M. Zeich, Executive Director

SUBJECT: Management Response (Assessment of Enterprise Risk Management Program Maturity Level)

We have reviewed the draft report of February 18, 2025, in which your team assessed the Commission's Enterprise Risk Management (ERM) program, and found that its maturity level is between emerging (level 2) and integrated (level 3). We appreciate the Office of Inspector General's commitment of time and resources to this maturity assessment.

We reviewed the report for technical accuracy and have no comments. The report made no recommendations. We concur with the report and will use it in addressing the ERM program maturity related recommendation from the 2024 ERM program audit accordingly.

KIMBERLY ZEICH Digitally signed by KIMBERLY ZEICH Date: 2025.02.18 08:44:00 -05'00'

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