U.S. ABILITYONE COMMISSION

Policy 51.703
Effective Date: November 29, 2021

TITLE: ENTERPRISE RISK MANAGEMENT PROGRAM

1. PURPOSE

To establish an Enterprise Risk Management (ERM) policy for the U.S. AbilityOne Commission, to outline the roles and responsibilities of Commission leadership related to ERM, and to describe the Commission's risk management processes and procedures.

2. APPLICABILITY

This policy applies to all Commission Directorates and components.

3. AUTHORITY

(a) 41 U.S.C §§ 8501-8506, Javits-Wagner-O'Day (JWOD) Act
(b) 41 Code of Federal Regulations (CFR) 51-2.2, Powers and Responsibilities
(c) Federal Manager's Financial Integrity Act (FMFIA) of 1982, Pub. L. 97-255 (codified at 31 U.S.C 3512) (Sept. 8, 1982).
(d) Government Performance Results Act (GPRA) Modernization Act of 2010, Pub. L. 111-352 (Jan. 4, 2011).

4. REFERENCES

(a) Office of Management and Budget (OMB), *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (July 2016)
(b) OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11, Part 6, §§ 260.29 – 260.32 (April 2021)
(c) Government Accountability Office, *Standards for Internal Control in the Federal Government*, GAO-14-704G (September 2014).

5. DEFINITIONS

(a) Executive Leadership Team (ELT): Led by the Executive Director and oversees the development and implementation of processes used to analyze, prioritize, and address risks across the Commission. These risks include operational and administrative consequences that could impede the Commission's ability to achieve its strategic objectives. The ELT is broadly responsible for ensuring that risks are managed to create value for agency stakeholders and in a manner consistent with established risk appetite and risk tolerance levels.

(b) Enterprise Risk Management (ERM): A comprehensive, agency-wide approach to risk

management joining organizational systems and processes together to improve decision-making quality and manage risks that may hinder the Commission's ability to achieve mission objectives.

(c) Enterprise Risk Management Steering Group (ERMSG): A directorate level working group that leads ERM activities under the supervision of the Chief Risk Officer (CRO) and oversees development and implementation of ERM processes the Commission uses to analyze, prioritize, and address potential or existing administrative or operational risks that could impact the Commission's ability to achieve its strategic objectives.

(d) Key Risk Indicator (KRI): Measurement warning of risk potential, or that a risk is occurring or has occurred.

(e) Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and associated consequences.

(f) Risk Analysis Integrated Project Teams: Responsible for assessing a defined risk, including identifying the risk's cross-functional, root causes and potential consequences, and coordinating with the ERMSG and Risk Owners to develop recommendations for risk response and monitoring plans.

(g) Risk Appetite: Amount and type of risk the Commission is willing to pursue or retain.

(h) Risk Owner: Person or organizational component provided risk management authority and accountable for managing assigned risks.

(i) Risk Issue: A potential or existing event or condition requiring implementation of risk management processes and procedures to ensure the Commission meets mission objectives.

6. RESPONSIBILITIES:

(a) The Executive Director is responsible for managing the Commission's ERM portfolio and accountable for effective ERM implementation. The Executive Director authorizes ERM policies and issues guidance.

(b) The CRO is responsible for designing, developing and implementing the Commission's ERM program. The CRO serves as the principal advisor to the Executive Director and Deputy Executive Director on all risk matters potentially impacting the Commission's mission performance.

(c) The ERMSG is responsible for:

(1) Leading ERM activities under the supervision of the CRO;

(2) Overseeing development and implementation of ERM processes the Commission uses to analyze, prioritize, and address potential or existing administrative or operational risks that could impact the Commission's ability to achieve its strategic objectives;

(3) Ensuring risks are managed to create external value in a manner consistent with established risk appetite and risk tolerances levels;

(4) Responding to changes in the risk environment the Commission identifies through risk events, changes to internal controls or significant changes to internal or external conditions that may or are expected to occur or have already occurred;

(5) Developing and maintaining ERM policies, processes, procedures, tools, mitigation and information systems;

(6) Leading the Commission's efforts in enterprise risk identification, assessment, prioritization, reporting, and monitoring;

(7) Overseeing enterprise-wide communications for gathering data and developing risk reports;

(8) Sharing information and providing subject matter expertise to support ERM program activities such as identification, validation and assessments of enterprise risks;

(9) Serving as the primary point of communication between the ERMSG and its respective ELT members.

(d) Agency Directors are responsible for:

(1) Serving as ultimate Risk Owners in accordance with the Commission's ERM policy;

(2) Ensuring their respective Directorate adopts and follows the Commission's ERM policy framework, and participates in enterprise-wide risk management efforts;

(3) Implementing consistent risk management practices aligned with ERM policy;

(4) Serving as primary representative to the Enterprise Risk Management Steering Group (ERMSG) and providing risk ownership for mitigation of risks throughout the ERM process, as necessary.

(5) Providing Directorate-level support in developing and implementing risk mitigation plans.

(6) Translating enterprise level risks into directorate level risks limits

(e) Risk Analysis Integrated Project Teams are responsible for assessing a defined risk, including identifying the risk's cross-functional, root causes and potential consequences, and coordinating with the ERMSG and Risk Owners to develop recommendations for risk response and monitoring plans.

7. POLICY:

The Commission's enduring mission is to create and expand employment opportunities for people who are blind or severely disabled. A risk management approach must support the Commission's ability to identify, analyze, and appropriately respond to strategic risks across the full spectrum of Commission activities. Accordingly, it is the Commission's policy, that:

(a) The CRO, working with the ELT, shall develop and implement the Commission's ERM framework across the organization. Through ERM, the Commission will:

(1) Provide a structured, disciplined, and consistent risk assessment approach aligned with OMB guidance memo 16-17, *Management's Responsibility for Enterprise Risk Management and Internal Control*, Circular No. A-123 (July 15, 2016);

(2) Identify strategic risks that threaten the Commission's achievement of long-term objectives and goals, and, through the ELT, manage those risks at the enterprise level;

(3) Ensure ERM maximizes the Commission's external value consistent with defined risk appetite and risk tolerance levels;

(4) Align internal strategies, processes, people, technology and information to support agile risk management;

(5) Provide greater risk transparency by improving understanding of interactions and relationships between risks in support of improved risk-based decision making;

(6) Establish clear accountability and ownership of risk.

(b) Risk management is central to the Commission's mission, vision and culture. All employees are expected to adopt the ERM principles developed in accordance with this policy, and apply the appropriate ERM processes, tools and techniques within their assigned responsibilities.

(c) Since the Commission creates value through expanding employment opportunities for people who are blind or have significant disabilities, the Commission seeks practical and cost-effective solutions to reducing administrative and operational risks.

(d) The Commission makes risk-informed decisions to achieve its mission within the parameters of its risk appetite:

(1) The Commission evaluates and manages program priority risks arising from program performance, budget, reputation, compliance and information technology security;

(2) The Commission considers the interconnected and interdependent relationship of its central and nonprofit agency oversight responsibilities when assessing risks and risk mitigation plans;

(3) The Commission recognizes the need to balance program effectiveness with operational efficiency, cost, industry vitality, and customer satisfaction by taking a systems approach to risk management;

(4) The Commission evaluates the highest risk scenarios and the effectiveness of controls to apply finite resources commensurate with the risk level;

(5) The Commission strikes a balance between countering known risks and hedging against unknown risks by using strategies such as continuous risk review, assessment and

mitigation planning within its ERM operational framework;

(6) The Commission maintains flexibility to focus resources on the basis of program performance results and operational effectiveness;

(7) The Commission takes decisive action responding to imminent threats with potentially damaging consequences, and maintaining program effectiveness may take precedence over other considerations;

(8) The Commission evaluates risk levels and implements risk responses and monitoring to bring the risk within tolerance without over-controlling non-program related enterprise risks;

(9) The Commission embraces innovation to address changes in employment opportunities of the blind and significantly disabled: understanding innovation requires experimentation and balancing timely deployment needs with appropriate program assessments.

8. EXCEPTION TO POLICY.

None.

9. PROCEDURES.

Detailed guidance may be found in the *Enterprise Risk Management Program Guide*, which is available on the Enterprise Risk Management SharePoint Site.

10. SUPERSESSION.

None.

This interim policy will be reviewed and revised as directed by OMB. It will be reissued not later than six months from the effective date.

APPROVED: Kimberly M. Zeich Date: 11/22/2021
Kimberly M. Zeich
Acting Executive Director