# MS 780 Enterprise Risk Management

**Effective Date:** April 29, 2024
**Responsible Office:** Office of the Director, Compliance and Risk Office
**Supersedes:** 07/09/19

Issuance Memo (07/09/2019)
Issuance Memo (04/29/2024)

**Table of Contents**



## 1.0 Purpose and Background

This Manual Section establishes the agency's Enterprise Risk Management (ERM) Program and defines the standards that will be used for managing "Risk" systematically across all strategy setting and operational activities of the agency.

The agency considers the management of Risk to be an integral part of good management and is committed to embedding "Risk Management" practices into agency processes so that Risk Management becomes a part of agency culture and is not viewed as an independent activity.

ERM Program activities focus on the agency's ability to manage uncertainty. The Risk Standards of the agency provide a structured and repeatable framework, principles, and process to guide the integration of Risk Management practices into the agency's day-to-day management activities.

## 2.0 Authorities and References

Implementation of the ERM Program and an agencywide system of Risk Management helps ensure compliance by the agency with federal requirements and guidance. These include:

(a) Federal Information Security Modernization Act of 2014 (FISMA);

(b) Office of Management and Budget Circular A-11 (2023) and A-123 Appendix A, (2018);

(c) White House Memorandum M-07-24 Updated Principles for Risk Analysis;

(d) White House Memorandum M-17-25 Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017);

(e) Government Performance and Results Modernization Act of 2010;

(f) Government Accountability Office Risk Management Framework (2016);

(g) Government Accountability Office Standards for Internal Control in the Federal Government (2014); and

(h) The International Organization for Standardization (ISO) 31000, *Risk Management – Guidelines* (2018).

## 3.0 Applicability

### 3.1 Scope

The Risk Management guidance, standards, and practices set forth in this policy can be integrated into all agency strategy setting, decision making, governance, and operational activities across all agency functions. The ERM Program will prioritize resources to address those enterprise-level Risk issues most likely to threaten agency-level objectives.

### 3.2 Exceptions

ERM Program resources and Risk Standards and practices will not be used in situations involving personal injury, loss of life, or instances where suspected violations of law have occurred.

## 4.0 Definitions

The agency's Risk Management framework employs the following standardized definitions:

(a) **Control:** Measure that maintains and/or modifies Risk.

(b) **Risk:** The effect of uncertainty on achievement of the objectives of an organization.

(c) **Risk-Informed:** An agency process, project, or activity that includes the use of a defined and systematic process; existence of a common understanding of context and objectives; robust consideration of Risk in achievement of objectives; and management of Risks consistent with agency "Risk Tolerance."

(d) **Risk Appetite:** The amount of various types of Risk that an organization is willing to incorporate within its operation.

(e) **Risk Assessment Process:** The overall process of "Risk Identification," "Risk Analysis," and "Risk Evaluation." (*See* subsection 5.1.)

(f) **Risk Consequence:** When the outcome of an event affects the achievement of objectives.

(g) **Risk Likelihood:** The chance that a Risk will occur.

(h) **Risk Management:** Coordinated activities to direct and control an organization with regard to Risk.

(i) **Risk Management Process:** The systematic application of management policies, procedures, and practices to activities involving communicating, consulting, establishing the context for, and identifying, analyzing, evaluating, treating, monitoring, and reviewing Risk.

(j) **Risk Standard:** Refers to ISO 31000, *Risk Management – Guidelines*, adopted by the agency in 2023.

(k) **Risk Tolerance:** An organization's or stakeholder's willingness to bear Risk after "Risk Treatment" (*see* subsection 5.1) to achieve objectives.

## 5.0 Policy

### 5.1 Standardized Risk Assessment Process

The agency will maintain a disciplined approach to Risk Management through the consistent application of a standardized Risk Management approach. The Risk Management framework establishes the principles and process to guide how the agency internalizes and integrates Risk Management practices into its day-to-day management activities. This iterative and scalable Risk Management Process includes the following steps:

(a) **Communication and Dialogue:** Communication and dialogue with internal and external stakeholders at each stage of the Risk Management Process.

(b) **Establishing Context:** Definition of relevant internal and external context and parameters when setting the scope and defining Risk criteria for the remaining Risk Management Process.

(c) **Risk Identification:** Generation of a comprehensive list of Risks that might enhance, prevent, degrade, or delay the achievement of objectives.

(d) **Risk Analysis:** Development of an understanding of Risks by considering their causes and sources, their positive and negative Consequences, and the Likelihood that consequences can occur while taking into account existing Risk Controls and their level of effectiveness.

(e) **Risk Evaluation:** Determination of which Risks need Risk Treatment (i.e., those that exceed Risk Tolerance) and in what order of priority.

(f) **Risk Treatment:** Selection of one or more options to modify unacceptable Risks. Options include changing the likelihood or consequence, avoiding the Risk, removing the Risk source, sharing the Risk with another party, seeking out the opportunity, or retaining the Risk by choice.

(g) **Monitoring and Review:** Ensuring that Risk Controls and Treatment measures are effective in both design and operation, identify new or emerging Risks or trends, assess changes in the internal and external environments that change the Risks, and implement lessons learned.

### 5.2 Risk-Informed Strategy Setting, Operations, and Decision Making

The Peace Corps' Risk-Informed strategy helps to set the foundation for ERM Program implementation activities, as Risk Management is geared towards managing Risks that can impact agency objectives. The agency sets its strategic and operational objectives, while managing Risks, in accordance with the following principles:

(a) Agency functions work to visibly internalize and integrate Risk Management practices into day-to-day operations and processes.

(b) The agency assesses Risks associated with changes in its internal and external operating environment when making Risk-based decisions.

(c) Non-routine or significant organizational decisions that do not fit into existing decision processes, are complex, or have the potential to materially affect existing agency systems, people, processes, or multiple organizations, are made in a Risk-Informed manner consistent with the agency Risk Management Process.

(d) Explicit consideration of Risk Appetite and Risk Tolerance is part of agency-level strategic and operational decision making.

(e) Risks associated with implementation of agency objectives are considered as part of the selection of objectives.

## 6.0 Roles and Responsibilities

### 6.1 Director

The Director is the ultimate authority for all ERM-related decisions and sets the Peace Corps' Risk Appetite. The Director shall receive recommendations on options for mitigating the agency's enterprise-level Risks from the Deputy Director and ERM Council.

### 6.2 Deputy Director

The Deputy Director:

(a) Oversees the unifying efforts across the agency to ensure that strategies and actions are informed by a common understanding of Risk, which is an essential requirement to inform priorities and allocate resources;

(b) Communicates the Peace Corps' Risk Appetite and ensures that adequate resources are in place to fully carry out this policy;

(c) Ensures that the Chief of Staff incorporates ERM into day-to-day operations;

(d) Convenes the ERM Council quarterly and ensures fulfillment of its duties and responsibilities, as set forth in the ERM Council Charter and By-Laws; and

(e) Serves as the Director's representative when convening the ERM Council, sharing relevant insights and guidance that help inform the ERM Council's deliberations.

### 6.3 Chief of Staff

The Chief of Staff:

(a) Ensures that Risk Management practices, at all levels, are integrated into informed-operational decision making and priority setting;

(b) Prioritizes the critical management responsibility of identifying potential Risks and avoidance or mitigation of those Risks; and

(c) In consultation with the Deputy Director and ERM Council, institutionalizes Risk Management agencywide into the Peace Corps by directing agency operating units to integrate the Risk Management Process into their day-to-day operations.

### 6.4 Enterprise Risk Management Council

The ERM Council serves as the senior advisory body to the Director and governance body regarding the Peace Corps' Risk Management framework, principles, and process. The ERM Council is governed by the ERM Council Charter and By-Laws. Regardless of individual title, position, or area of responsibility or expertise, ERM Council members maintain an objective,

enterprise-level view of achieving the Peace Corps' mission and objectives when reviewing, evaluating, and monitoring opportunity and Risk issues brought to the Council for deliberation or decision. The ERM Council, primarily composed of senior level representatives, does the following:

(a) Provides policy and management oversight and advice with respect to the coordinated approach to ERM Program implementation and operations;

(b) Facilitates ERM Program governance and consideration of Risk as an element of the agency's decision-making; and

(c) Informs Peace Corps management of progress towards ERM Program maturity and the efficacy of current policy.

### 6.5 Enterprise Risk Management Council Secretariat

The ERM Council Secretariat is appointed by the ERM Council Chair and serves as the advisory body to the ERM Program implementation efforts. The ERM Council Secretariat:

(a) Provides advice, recommendations, and feedback to the Compliance and Risk Office related to ERM Program implementation activities, conducting specific Risk assessments, or leading specific Risk Management projects;

(b) Provides review of Risk Management outputs in advance of ERM Council discussions; and

(c) Performs other tasks as may be delegated by the ERM Council.

### 6.6 Chief Compliance and Risk Officer

The Chief Compliance and Risk Officer:

(a) Provides oversight and direction to the Risk Officer and to the day-to-day ERM Program implementation activities;

(b) Communicates new, emerging, or significant Risk issues to executive leadership as operational conditions evolve;

(c) Works to coordinate the integration of Risk Management practices into agency management activities, internal Control function efforts, and audit activities;

(d) Serves as a Risk Management advisor to the Chief of Staff and Deputy Director, and other staff, on the integration of Risk Management practices into the Peace Corps' day-to-day business operations and decision-making;

(e) Serves on the Peace Corps' ERM Council and the ERM Council Secretariat; and

(f) Provides recommendations of the ERM Council to the Deputy Director, in consultation with the ERM Council and Chief of Staff, as guided by the ERM Council Charter and By-Laws.

### 6.7 Risk Officer

The Risk Officer:

(a) Ensures consistent and coordinated implementation of the Peace Corps' Risk Management framework and process;

(b) Leads the development, administration, interpretation, and communication of Risk Management policies, procedures, guidance, and resources;

(c) Conducts and facilitates Risk assessments on key strategies, projects, or initiatives;

(d) Provides Risk Management advice, consultation, and training to agency staff and leadership;

(e) Provides complete written minutes of the proceedings, deliberations, and recommendations to the ERM Council, as guided by the ERM Council Charter and By-Laws;

(f) Serves as a strategic advisor to agency leadership and staff on the integration of Risk Management practices into the Peace Corps' day-to-day business operations and decision-making;

(g) Coordinates the activities of the Peace Corps' ERM Council and ERM Council Secretariat; and

(h) Organizes ERM Council and ERM Council Secretariat meetings, including preparing the meeting agendas, distributing briefing papers on agenda items, maintaining meeting minutes, and maintaining an archive of ERM Council decisions.

### 6.8 Peace Corps Operating Units

Risk Management must be a visible and integral part of the Peace Corps' culture, allowing the agency to fulfill its mission and strategic objectives more effectively. As directed by the Chief of Staff, offices are responsible for ensuring that their day-to-day operations are Risk-Informed.

Managers and supervisors must ensure that those with Risk Management responsibilities within their operating units have access to Risk Management guidance and resources and that all agency employees are aware of and follow Risk Management policies, framework, and processes.

### 6.9 Office of Chief Financial Officer

The Office of the Chief Financial Officer (OCFO) oversees, assesses, and tests the internal controls over financial reporting as part of the requirements outlined in Appendix A of OMB Circular A-123.

### 6.10 Office of the Chief Information Officer

The Office of the Chief Information Officer (OCIO) establishes, implements, and ensures compliance with an agencywide information security program consistent with the Federal Information Security Modernization Act (FISMA).

### 6.11 Office of the Safety and Security

The Office of Safety and Security (OSS) establishes, implements, and ensures compliance with an agencywide Classified National Security Information (CNSI) Program consistent with the Office of the Director of National Intelligence, Security Executive Agent Directives.

### 6.12 All Employees

All executives, managers, and staff have an important role in managing Risk across the agency and are expected to make and support Risk-Informed decisions. To the extent that an employee becomes aware of what appears to be a significant Risk-related issue that they believe could jeopardize the agency's success, the employee should notify a supervisor, the Chief Compliance and Risk Officer, or the Risk Officer so that appropriate action may be taken.

## 7.0 Enterprise Risk Management Program Functions

The ERM Program functions are as follows:

(a) **Agency-Level Risk Profile:** Maintains an agencywide view of the agency's most significant Risks threatening agencywide objectives to help inform agencywide strategic and operational priorities and budget resource allocation decisions, communicate priorities, and ensure that activities at the office-level are aligned with agency priorities.

(b) **Office-Level Risk Registers:** Maintains logs of office-level Risks that each office uses proactively to identify, analyze, and manage Risks in a disciplined way. Risk registers help to embed Risk Management practices into existing agency processes in a disciplined and repeatable manner, provide structured opportunities to proactively identify new and emerging Risks, and inform office-level plans and priorities.

(c) **Risk Appetite:** Ensures that the agency clearly defines the amount and type of Risk that the agency is willing to pursue or retain in pursuit of its mission. Risk Appetite is established by the Director and serves as the guidepost to set strategy and select objectives.

(d) **Risk Consultation and Training:** Provide Risk Management consultation and advice to leadership as needed or provide Risk Management response to emerging Risk issues. Provide Risk Management training to staff and leaders.

## 8.0 Effective Date

The effective date of this Manual Section is the date of issuance