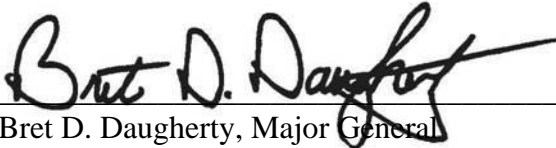




## Department Policy No. RSM-601-03

<b>Subject:</b>	Enterprise Risk Management Policy
<b>Authorizing Source:</b>	<a href="#">Executive Order 16-06</a> <a href="#">RCW 43.19.760</a> : Risk Management Principles <a href="#">RCW 43.19.763</a> : Risk Management Definitions <a href="#">RCW 43.19.781</a> : Safety and Loss Control Program <a href="#">SAAM 20.20</a> : Internal Control Environment
<b>Information Contact:</b>	Risk Manager Building #1, Camp Murray (253) 512-7381
<b>Effective Date:</b>	May 15, 2011
<b>Mandatory Review Date:</b>	May 30, 2027
<b>Revised:</b>	May 30, 2023
<b>Approved By:</b>	 Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

### Purpose

The Washington Military Department (WMD) has established an Enterprise Risk Management (ERM) program that provides a framework to proactively identify, assess, and manage risks that may affect the agency's ability to achieve its mission, goals, and strategic objectives per the Governor's Executive Order 16-06.

### Scope

This policy applies to all state employees of the WMD, including Washington Army and Air National Guard members on State Active Duty.

### Policy

WMD proactively identifies, assesses, and responds to risks that may affect our ability to provide our core mission services and the achievement of our strategic and performance-based objectives and their intended outcomes.

WMD uses a consistent, integrated, and transparent ERM approach to support informed decision-making and resource allocation at both the strategic and operational levels.

WMD will provide training and apply ERM best practices to identify and manage internal and external risk to protect resources, employees, contract staff, and the public. ERM best practices will be used as an integral part of considering risk in the decision-making process through identifying risks and opportunities across all divisions, facilities, programs, and areas of operation. Once a risk has been identified and prioritized, the agency will develop, implement, and monitor risk treatment strategies.

## **Roles and Responsibilities**

### **1. Agency Director**

- a. Leads, supports, and ensures commitment to implementing the ERM ISO 31000 Purpose, Principles, Framework and Risk Management Process.
- b. Establishes and communicates their risk appetite and the organization's risk tolerance to all employees to support efficient and effective risk mitigation.
- c. Makes a commitment to adopting and integrating ERM into the organizational culture.
- d. Ensures appropriate allocation of resources to support risk management activities.

### **2. Risk Oversight Committee (ROC)**

- a. The ROC provides management support and commitment to ERM.
- b. The ROC will:
  - (1) Support an enterprise-wide commitment to risk management across the entire organization, from front line employees to management and from management to employees.
  - (2) Participate in risk identification and risk prioritization.
    - i. Risks will be prioritized at an enterprise-wide level by analyzing the likelihood and impact of each risk.
    - ii. Identify emerging risks and any significant changes to current risks.
    - iii. Ensure the reallocation of resources for managing risks.
- c. Create a communication channel for risk owners of the higher scored risks to report on their risks quarterly to the ROC.
- d. Include risk consideration as an integral part of the organization's decision-making process.
- e. Support education, training and information sharing on ERM policies and procedures to promote enterprise-wide awareness.

### **3. Executive Risk Owners**

- a. For risks that fall within their purview, executive risk owners will work with risk owners to:
  - (1) Review, approve and support the implementation of risk mitigation strategies.
  - (2) Review mitigation strategy effectiveness for risks.
  - (3) Ensure the reallocation resources for managing risks.
  - (4) Create a communication channel for risk owners to report on their risks regularly.

### **4. Risk Manager**

- a. The risk manager coordinates and facilitates the enterprise-wide effort necessary to identify, evaluate, mitigate, and monitor the agency's strategic/operational, legal/compliance, financial, reputational, health/safety and employment risks.

- b. The risk manager will:
  - (1) Develop ERM tools, practices, and processes to identify, analyze and report enterprise-wide, strategic risks according to this policy and the ISO 31000 ERM framework.
  - (2) The risk manager will, by using the Origami ERM module, monitor and facilitate the management of risks by:
    - i. Ensuring the completion of quarterly updates of the highest scored risks.
    - ii. Ensuring the completion of the semi-annual updates of identified risks.
    - iii. Ensuring the completion of the semi-annual prioritization of identified risks.
    - iv. Attesting to compliance with the Governor's Executive Order 16-06 annually.
    - v. Managing the risk register in the Origami ERM Module.
  - (3) Support employee awareness and understanding of ERM through education, training, and information sharing.
  - (4) Coordinate reporting on risk treatment activities by risk owners to the leadership team as required.
  - (5) Report quarterly to the ROC on the management of risks, loss history, and emerging risks.
  - (6) Annually review and recommend revisions to this policy.

#### 5. Risk Owners

- a. Develop and implement mitigation plans and controls for assigned risks.
- b. Monitor assigned risks to ensure the mitigation strategies are controlling the risks.
- c. For risk owners with the highest scored risks:
  - (1) Update risks quarterly using the Origami ERM module as assigned by the risk manager.
  - (2) Report the status of assigned risks – controls, gap analysis, mitigation progress and risk metrics - to the ROC quarterly.
- d. For all other risks owners:
  - (1) Update risks semi-annually using the Origami ERM module as assigned by the risk manager.
  - (2) Report the status of assigned risks – controls, gap analysis, mitigation progress and risk metrics - to the executive owner and/or leadership team as needed.

#### 6. Managers and Supervisors

- a. Managers and supervisors apply ERM in all aspects of operations and actions.
- b. Managers and supervisors will:
  - (1) Set the standards and expectations of staff with respect to addressing risks. Ensure internal control processes are implemented, maintained, and monitored to manage risk.
  - (2) Support ERM training for all employees.

#### 7. All Employees

- a. All employees are responsible for understanding and supporting the agency's efforts to identify, eliminate or manage risk.
- b. Employees will identify and communicate risks to their supervisor or the risk manager.

## Definitions

**Enterprise risk management:** the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk. ISO 31000 is the international standard for the practice of risk management. It is an enterprise-wide approach that proactively identifies, assesses, and prioritizes strategic risks, followed by the allocation of resources to minimize, monitor, and control the likelihood and impact of risks occurring, or to maximize opportunities.

**Executive risk owner:** the executive or leadership team member who has oversight of the risk. This means that the risk resides in a division/program, etc., for which the executive owner is responsible.

**Origami ERM Module:** Allows risk managers a software solution to streamline all ERM processes. This module's data includes a list of identified risks, individual risk rating and score, current controls, treatment plan, risk metrics, and who is accountable for managing the risk. This module is owned and maintained by the state's Department of Enterprise Services

**Risk identification:** the process of identifying risks that might enable or impede the agency's ability to provide its core mission services or meet its strategic objectives, i.e., brainstorming session.

**Risk owner:** the person with the authority and accountability for managing a particular risk.

**Risk prioritization:** the process of evaluating identified risks to determine the likelihood and impact of each risk, resulting in a risk score and rating.