Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No 09.13

Subject: Enterprise Risk Management

Information contact:
Chief Risk Officer
MS 45020
Tel: (360) 902-7794

Authorizing sources:
Executive Order 16-06
SAAM 20.20 (July 1, 2017)
RCW 43.19.760
RCW 43.19.763
RCW 43.19.781

Resources:
Risk Management Basics
Department of Enterprise Services
Enterprise Risk Management Training Template
(Department of Enterprise Services)

Effective date: December 15, 2011

Revised: October 2, 2020

Approved by: **Original signed by Lori Melchiori**
Senior Director, Office of Policy and Rules

Purpose

This policy is to ensure DSHS uses the Enterprise Risk Management (ERM) framework to assess and manage potential risks and opportunities that could affect the ability of DSHS to achieve its mission, vision, and goals.

This policy requires that DSHS:

- Implement and utilize ERM assessment systems to identify the department's potential risk exposure in such areas as: routine operations, capital holdings, regulatory compliance, financial stewardship, organizational reputation, and staff safety;
- Determine the potential impacts of risks and prioritize them with consideration to the department's strategic plans, budget, and reputation;
- Adopt policies, plans, controls, and practices to mitigate identified risks;
- Delegate responsibilities appropriately in order to effectively control risks; and
- Track, measure, and review risk issues, mitigation strategies and their outcomes for effectiveness.

Scope

This policy applies to all Department of Social and Health Services organizational units.

Definitions

Enterprise risk management (ERM) is an integrated approach to identify, understand, manage, and mitigate risks an organization may face across all agency programs. The primary purpose of ERM is to inform and improve decision-making throughout an organization.

Chief risk officer (CRO) is the executive level position delegated to develop and ensure the integrity and operation of risk management practice including assessing and mitigating risks across the department.

Risk is the effect of uncertainty on the department's ability to achieve its objectives, or successfully achieve its strategic purposes.

Risk assessment is an ongoing process that includes identifying, analyzing, and evaluating risks and deciding how to respond to them.

Risk management is the systematic application of policies, procedures, and practices of identifying, analyzing, assessing, monitoring, and mitigating risks.

Risk register is a document that details the risk assessment by providing a list of high-priority risks to reaching the goal and an overview of how each will be handled.

Risk response means the action(s) taken to address an identified risk including:

- Avoidance (usually by discontinuing the activity)
- Accepting and monitoring (this should include setting a threshold to begin treatment)
- Reducing the likelihood/impact (reducing the conditions or occurrences)
- Transfer (e.g. through insurance or a contract)

Policy

A. The department is committed to adopting and maintaining ERM processes to:

1. Guide business planning in all its organizational units;

2. Track significant risk assessment and mitigation activities using data, reports, and a risk register;

3. Monitor and assign accountability of risk mitigation practices;

4. Monitor asset protection practices and outcomes; and

5. Monitor environmental, health, and safety processes, practices, and outcomes.

B. The chief risk officer is responsible for coordinating the department's ERM activities and keeping the secretary and executive leadership team advised of potential risk issues that could prove significant to the department.

C. Administrations, divisions, and offices within the department are expected to develop and employ ERM practices throughout their operations and work cooperatively with the enterprise risk management office (ERMO) in that effort. Accordingly, each administration must:

1. Designate a representative to participate with ERMO on risk management planning, training, and implementation for the department as well as participate in quarterly agency risk management meetings.

2. Communicate significant categories or types of risks associated with its operations to ERMO using a risk register.

3. Ensure that their administration's internal risk management systems, policies, and protocols (including training plans) support and promote the department-wide ERM concepts and monitoring tools.

D. ERMO must:

1. Research and recommend ERM best practices for department program adoption and implementation;

2. Communicate significant categories or types of risks associated with its operations to DES risk management, as appropriate, using a risk register;

3. Prepare, in collaboration with department administrations, divisions, and offices, an agency risk assessment tool and process;

4. Hold quarterly agency risk management meetings with administration representatives;

5. Report analyses, risk status, and risk reduction or mitigation outcomes quarterly, and as required to the department's executive leadership team; and

6. Develop and provide opportunities for education, training, and exposure to ERM to support workforce understanding of the process, and embed ERM principles when making decisions at all levels of the agency.