CASCADIA COLLEGE
BOTHELL • OUR COMMUNITY'S COLLEGE

Board Policy: Enterprise Risk Management Policy	Policy Number: BP06:04.10
Article: 6.) Facilities Section: 4.) Risk Management	Adopted by the BOT: 10/19/22
Applicable WAC/RCW: RCW 43.19.760, 43.19.763, 43.19.781 SAAM 20.20	

BP06:04.10 Enterprise Risk Management

Cascadia College 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.

Cascadia College will provide management support and commitment to safety and loss control, and develop awareness of ERM through education, training, and information sharing per RCW 43.19.760, the Governor's Executive Order 16-06 and ISO 31000.

SCOPE

This policy applies to all *Cascadia College* employees and organizational units.

POLICY

Cascadia College 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. ***Cascadia College*** uses Origami Enterprise Risk Management software to provide a consistent, integrated, and transparent enterprise risk management (ERM) approach to support informed decision-making and resource allocation at both the strategic and operational levels.

Cascadia College 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 *Cascadia College* 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. **Vice President for Administrative Services**
    - Leads, supports, and ensures commitment to implementing the ERM ISO 31000 Purpose, Principles, Framework and Risk Management Process.
    - Establishes and communicates the organization’s risk tolerance to all employees to support efficient and effective risk mitigation.
    - Makes a commitment to adopting and integrating ERM into the organizational culture.
    - Ensures appropriate allocation of resources to support risk management activities.

2. **Leadership Team**
    - The leadership team provides management support and commitment to ERM.
    - The leadership team will:
        - Support an enterprise-wide commitment to risk management across the entire organization, from front line employees to management and from management to employees.
        - Participate in risk identification and risk prioritization sessions semi-annually.
            - Risks will be prioritized at an enterprise-wide level by analyzing the likelihood and impact of each risk.
            - Identify emerging risks and any significant changes with risks.
            - Ensure the reallocation resources for managing risks
            - See page 4 of this policy for the method, timeline and scoring criteria used for identifying and prioritizing risks.
        - Create a communication channel for risk owners of the highest scored risks to report on their risks quarterly to the leadership team.
        - Include risk consideration as an integral part of the organization’s decision-making process.
        - Support education, training and information sharing on ERM policies and procedures to promote enterprise-wide awareness.

3. **Executive Risk Owners**
    - For risks that fall within their purview, the leadership team will work with risk owners to:
        - Review, approve and support the implementation of risk mitigation strategies.
        - Review mitigation strategy effectiveness for risks.
        - Ensure the reallocation resources for managing risks.
        - Create a communication channel for risk owners to report on their risks regularly.

4. **Risk Manager**
    - 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.

- The risk manager will:
    - 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.
    - The risk manager will, by using the Origami ERM module, monitor and facilitate the management of risks by:
        - Ensuring the completion of quarterly updates of the highest scored risks.
        - Ensuring the completion of the semi-annual updates of identified risks.
        - Ensuring the completion of the semi-annual prioritization of identified risks.
        - Attesting to compliance with the Governor's Executive Order 16-06 annually.
        - Managing the risk register in the Origami ERM Module.
    - Support employee awareness and understanding of ERM through education, training, and information sharing.
    - Coordinate reporting on risk treatment activities by risk owners to the leadership team as required.
    - Report quarterly to the Leadership Team on the management of risks, loss history, and emerging risks.
    - Annually review and recommend revisions to this policy.

5. Risk Owners

- Develop and implement mitigation plans and controls for assigned risks.
- Monitor assigned risks to ensure the mitigation strategies are controlling the risks.
- For risk owners with the highest scored risks:
    - Update risks quarterly using the Origami ERM module as assigned by the risk manager.
    - Report the status of assigned risks – controls, gap analysis, mitigation progress and risk metrics - to the leadership team quarterly.
- For all other risks owners:
    - Update risks semi-annually using the Origami ERM module as assigned by the risk manager.
    - 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

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

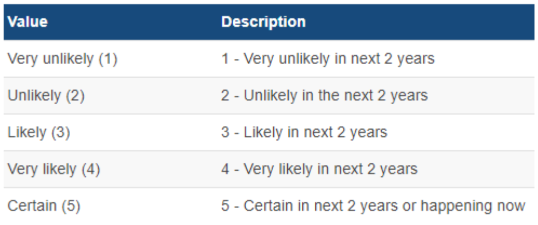
7. **All Employees**
   - All employees are responsible for understanding and supporting the agency's efforts to identify, eliminate or manage risk.
   - Employees will identify and communicate risks to their supervisor or the Risk Manager.

PROCEDURES

METHOD, TIMELINE AND SCORING CRITERIA FOR IDENTIFY AND PRIORITIZING RISKS

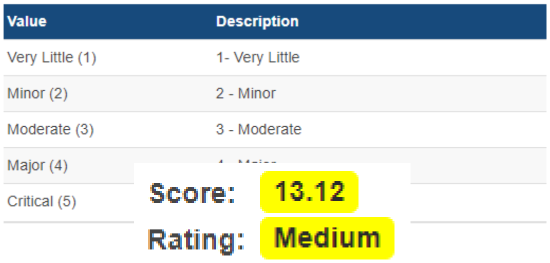
1. Risk identification will occur in a brainstorming session with the executive team/leadership team. After the initial session, new risks will be identified in a brainstorming session semi-annually, prior to the semi-annual risk prioritization session.
2. Risk Prioritization will occur after risks have been identified. The Origami ERM module ERM Plan will be used to prioritize (score) the identified risks.
   - Risks are scored by determining the likelihood of each risk occurring within the next two years, and by determining the impact of the risk if it did occur.
     - Likelihood and Impact are scored as shown below:

Likelihood Scoring



Value	Description
Very unlikely (1)	1 - Very unlikely in next 2 years
Unlikely (2)	2 - Unlikely in the next 2 years
Likely (3)	3 - Likely in next 2 years
Very likely (4)	4 - Very likely in next 2 years
Certain (5)	5 - Certain in next 2 years or happening now

Impact Scoring



Value	Description
Very Little (1)	1- Very Little
Minor (2)	2 - Minor
Moderate (3)	3 - Moderate
Major (4)	4 - Major
Critical (5)	

Score: 13.12

Rating: Medium

   - All leaders score ALL risks. The likelihood scores are averaged, and the impact scores are averaged; then the average likelihood score is multiplied by the average impact score, resulting in a final risk rating and risk score between 1-25.

For example: 3.2 x 4.1 =The rating scale for risk scores is shown in the table below:

1-5	Low	🟩
6-10	Medium Low	🟩
11-15	Medium	🟨
16-20	Medium High	🟧
21-21	High	🟥

DEFINITIONS

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

Origami ERM Module is a list of identified risks, the risk rating and score of each risk, the current controls, treatment plan, risk metrics and who is accountable for managing the risk. This module, owned and maintained by the Department of Enterprise Services, allows risk managers a software solution to streamlining all ERM processes.

Risk identification means 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 means the person with the authority and accountability for managing a particular risk.

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