Policy Name:	Enterprise Risk Management Policy
Originating/Responsible Department:	Vice-President: People, Finance, Operations
Approval Authority:	Board of Governors
Date of Original Policy:	November 2008
Last Updated:	December 2025
Mandatory Revision Date:	December 2030
Contact:	Associate Vice President, Department of Risk Management

Policy

The Enterprise Risk Management policy affirms Carleton University's commitment to risk management and articulates the role that the Enterprise Risk Management Framework plays in determining the university's Risk Appetite, as well as its application in day-to-day operations. This policy outlines key elements of Enterprise Risk Management and the university's responsibility to:

- Manage risk and ensure alignment with objectives, other policies and applicable legal requirements, which also follow the ISO 31000 standard.
- Integrate risk management into the overall culture of the organization.
- Understand the interaction of risk management with core business activities and decision-making.
- Identify authorities, responsibilities, and accountability.
- Provide the necessary resources.

Definitions

Enterprise Risk – The possibility that events will occur and affect the achievement of strategy and business objectives.

Enterprise Risk Management – The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk and create, preserve and realize value.

Enterprise Risk Management Framework – A set of components that provide the foundations and organizational arrangement for designing, implementing, monitoring, reviewing, communicating and continuously improving the management of risk throughout the university.

Risk Appetite – The types and amount of risk the university is willing to accept.

- **Conservative – willingness to accept minimal risk and comfortable with lower but more predictable outcomes.**
- **Balanced – willing to accept some risk to achieve strategic goals but not comfortable with high levels of uncertainty or volatility.**
- **Entrepreneurial – comfortable with uncertainty and volatility and are often early adopters of new ideas and ventures.**

Risk Owners – The individuals who have the accountability and authority to manage the applicable risk.

Risk Treatment – The process to modify risk and may include accepting, avoiding, transferring, or mitigating the impact of the risk.

Key Risk Indicators – a measure to indicate the potential presence, level or trend of risk.

Purpose

Integrating Enterprise Risk Management practices across Carleton enhances decision-making in governance, strategy, objective-setting, and daily operations. This approach fosters continuous improvement by aligning strategy and business objectives with risk management. The diligence involved in Enterprise Risk Management provides a clear path for creating, preserving, and realizing value.

A robust risk management culture supports Carleton's core mission to advance learning through teaching, study, and research, and a vision to be a leader in collaborative and interdisciplinary education. Carleton's commitment to a risk-aware culture emphasizes the importance of managing risk and promotes the transparent and timely flow of risk information. This is achieved without assigning blame, but with a focus on understanding, accountability, and continuous improvement.

Scope

This policy applies to all Board of Governors members, faculty, staff, students, visitors and contractors.

Responsibility for identifying and managing the risks of the university lies with the risk owners of the institution. Academic and administrative leadership are responsible for ensuring compliance with university policies and applicable legislation and regulation. Leadership also has the responsibility to identify, evaluate and manage enterprise risks and bring emerging risks to the President's attention.

The Enterprise Risk Management Framework provides the process and guidelines for enterprise risks, as well as for the creation of risk mitigation strategies. The Framework also informs the internal auditing process at the university and helps to identify which operational areas could be audited for the purpose of providing assurance on the effectiveness of internal

controls and continuous improvement.

The Department of Risk Management is responsible for the Enterprise Risk Management Framework.

Procedures

The university has adopted an Enterprise Risk Management Framework, and procedures to ensure that operational managers apply due diligence, demonstrate due care, comply with applicable laws and regulations and take the appropriate level of risk when making decisions.

There are three main components to enterprise risk management: principles, risk assessment, and framework.

1. **Enterprise Risk Management (ERM) Principles**

   The following ERM principles are supported by this policy:

   - Create awareness of the business risks that are associated with the operations of the university;
   - Create awareness of the key enterprise risks that the university faces;
   - Apply due diligence in decision-making;
   - Exercise an appropriate level of care in daily operations;
   - Apply intelligent risk-taking in the pursuit of new ideas and innovation; and
   - Apply legal and statutory compliance as a minimum standard.

2. **Enterprise Risk Management (Risk Assessment)**

   The enterprise risk management process is linked directly to the university's strategic planning process. The Associate Vice President, Department of Risk Management, is responsible for the development and implementation of the enterprise risk management framework. It is also the responsibility of the Associate Vice President, Department of Risk Management to communicate the key enterprise risks identified as part of the enterprise risk management process to stakeholders, such as senior management and the Board of Governors.

3. **Enterprise Risk Management Framework**

   Carleton's Enterprise Risk Management Framework provides a foundational and organizational structure for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization. The Audit and Risk Committee is responsible for reviewing and approving the Enterprise Risk Management Framework for the University every five years.

Internal Audit

Internal Audit plays a role in risk awareness to evaluate the risk management processes of the university. It also provides support in risk identification by determining the effectiveness of internal controls and identifying risks not addressed by current internal controls. Internal Audit also uses the enterprise risk management process as a tool to identify areas which should be audited. Internal Auditors report observations and recommendations to the Audit and Risk Committee. The Audit and Risk Committee will receive reports on the status of implementation of all outstanding internal audit recommendations.

Insurance

The following guidelines ensure that the proper insurance coverage is in place to meet the risk financing objectives:

i) The procurement of all insurance coverage and products must be arranged or approved by the Department of Risk Management.

ii) The university shall purchase insurance to protect against catastrophic loss to its physical, financial and other assets. It shall also use insurance as its method of risk financing to protect its Board of Governors, officers, supervisors, employees, volunteers and students, acting in good faith, against liability arising out of their duties as officers, directors, supervisors, employees and students at the university.

iii) The payment of deductibles and non-insured losses (e.g. below the deductible amount) shall be the responsibility of the department suffering from the loss. Personal property of faculty, staff and students is not covered by the university's insurance policies.

iv) It is the responsibility of each department manager to advise the Department of Risk Management of changes in programs, activities, or assets, which may affect insurance coverage in place.

Reporting of Potential Proceedings and Insurance Claims

It is the responsibility of all members of the community to report any pending or actual claim, lawsuit, or regulatory proceeding against the university to the Office of University Legal Services and the Associate Vice President, Department of Risk Management as soon as they become aware of a claim or possible claim. If insurance coverage applies, the appropriate insurer will be engaged. If no coverage exists, the Office of University Legal Services will manage and supervise the university's response or defense to the proceeding and retain external counsel as may be appropriate.

No employee shall settle a claim, regulatory proceeding or legal action against the university without consulting with Office of University Legal Services and receiving the approval of the President and/or the appropriate Vice-President responsible for the operations from which the claim, regulatory proceeding or legal action originates.

Required Insurance and Indemnity Provisions in Contracts

The university shall require all individuals, groups, tenants and independent contractors using Carleton University facilities and/or entering into contracts (including all purchase orders) with the university to hold the university harmless from all claims for bodily injury or property damage and provide proof of General Liability insurance in an amount of not less than $5 million, including adding Carleton University as an additional insured to their policy. In rare and extenuating circumstances, the Department of Risk Management may alter or waive these requirements.

Roles and Responsibilities

President: Fosters a strong risk management culture which provides general risk management oversight to ensure Enterprise Risk Management adoption throughout the university and assesses top risks and action plans and reviews/approves major risk treatment options.

Vice-Presidents: The Vice-Presidents are accountable to the President for risk management and for developing and implementing policies and procedures for risk management. They also ensure that recommendations and directions of the Board of Governors, President, and Internal and External Auditor, with respect to risk management are acted upon and will be the risk owners within their responsibilities and level of authority. All information on enterprise risk management and mitigation strategies should be promptly presented to the responsible Vice-President.

Board of Governors & Audit and Risk: The Board of Governors has the primary responsibility for risk oversight and a fiduciary duty to act in the best interest of Carleton University, including conducting reviews of enterprise risk management practices and approving the Enterprise Risk Management policy. While the full board oversees risk, day-to-day risk management is handled by management.

The Audit and Risk Committee will review and recommend approval of Risk Appetite statements to the Board of Governors. Additionally, recommendations from internal and external auditors regarding risk management must be identified and acted upon.

Administration and Academic Leaders: Administration and academic leaders of the university, and its controlled entities, are responsible for incorporating risk management into their standard management practices by identifying and determining appropriate actions to address operational risks within their area of responsibility in accordance with university policies and procedures.

Associate Vice President, Department of Risk Management: Responsibility for overall risk management at the university and as such is responsible for developing the risk management framework and policies that allow the university to manage risk in a structured way and promote a strong risk management culture at Carleton University.

All faculty, staff and contractors: have a shared responsibility and play an integral role in identifying, assessing, and treating risks to ensure the achievement and sustainability of Carleton University's academic mission.

Contacts:
Vice-President (People, Finance & and Operations)
Associate Vice President, Department of Risk Management
Office of University Legal Services
University Governance Secretariat

Links to related Policies:
Signing Authorities Policy
Legal Advice and Charges Policy
Financial Fraud Prevention and Reporting Policy
Data Protection and Risk Management Policy
University Information Technology (IT) Security Policy
Business Continuity and Resilience Policy