POLICY NAME	ENTERPRISE RISK MANAGEMENT POLICY
Approving Body	Board of Governors
Initial Approval Date	November 30, 2010
Date of last review	February 13, 2020
Date of next review	February 2025
Executive Sponsor	President and Vice-Chancellor

Related Documents	N/A

PURPOSE

1. The purpose of the Enterprise Risk Management Policy ("ERM Policy") is to articulate McGill University's overarching approach to entity-wide risk management and its activities, and to define roles and responsibilities for the establishment and maintenance of McGill's ERM program, as well as set out a common language toward addressing University-wide risks and mitigation.

ERM at McGill

2. Enterprise Risk Management Policy ("ERM") is a program that enables organizations to identify, assess, mitigate and manage potential risks in a comprehensive, methodical, and transparent way, using a common set of definitions and metrics.

ERM provides a structured, consistent, and continuous process for the early and proactive identification, and reporting of material risks and opportunities to the senior administration and the Board of Governors.

McGill's ERM program enhances its ability to achieve its mission, vision, and strategic objectives. ERM aims to strengthen McGill's competitive position by fostering an institution-wide culture of risk and opportunity awareness.

3. The University's ERM program aims to:

3.1 Provide McGill with a consolidated, comprehensive and holistic approach to identifying its most significant risks as an organization;

3.2 Clarify ERM roles and responsibilities of the various key stakeholders;

3.3 Enable a systematic and consistent approach to identifying, assessing, and managing risks with a common language and framework in order to facilitate the achievement of McGill's objectives and planned results;

3.4 Make risk management integral to McGill's culture, strategic planning, and decision-making;

3.5 Facilitate risk-informed decisions when setting objectives, selecting and managing the most appropriate course of action, and evaluating results;

3.6 Maintain forward-looking rather than reactive risk management by encouraging well planned and well managed risk-taking;

3.7 Facilitate a change in organizational culture to enhance risk management practices; and,

3.8 Provide assurance to stakeholders that McGill's objectives will be met, key risks will be better managed, and results will be demonstrated.

SCOPE

4. As a fundamental principle of ERM, the ERM Policy applies to all employees across all faculties, departments, units and activities of the University, including academic, research, administration and support activities. It also applies to the Board of Governors and to the Board's committees.

ERM DEFINITIONS

5. The University has adopted key definitions guided by two risk frameworks (ISO 31000 and COSO):

5.1 **Risk:** The uncertainty of an event occurring (or failing to occur) which could have an adverse impact on the achievement of operational and strategic objectives.

5.2 **Inherent Risk:** The risk of an event occurring (or failing to occur) in the absence of a risk management framework and/or internal control(s) in place to mitigate the risk.

5.3 **Residual Risk:** The remaining risk of an event occurring (or failing to occur) after considering a risk management framework and/or internal control(s) in place to mitigate the risk.

5.4 **Risk Appetite:** The overall level of risk an organization is willing to accept given its capabilities and the expectations of its stakeholders.

5.5 **Enterprise Risk Management (ERM):** A coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.

5.6 **Risk Management Framework:** Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

5.7 **Enterprise Risk Assessment (ERA):** A systematic and forward-looking analysis of the impact and likelihood of potential future events on the achievement of an institution's objectives within a stated time horizon.

The risk assessment criteria are defined as followed:

Likelihood: The probability that a given risk will occur based on McGill's and other Higher Education Institutions' past experience.

Impact: The effect of a risk occurring which can include financial, reputational, regulatory, safety, environmental, operational, and other losses.

5.8 **Contributing Factors:** Events or circumstances within the University's context that increase the likelihood that a risk will materialize and/or increase its impact.

5.9 **Risk Response:** The process of selecting and implementing one or more risk treatment options.

5.10 **Risk Owner:** A person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

5.11 **Risk Action Owner:** A person that has been given the authority by the Risk Owner to execute the risk mitigating response.

5.12 **Control:** Any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk.

There are two types of controls:

Preventive Control: A control procedure designed to prevent an adverse event, error or fraud.

Detective Control: A control designed to monitor the achievement of the relevant process objective, including identifying an adverse event, error or fraud, which has occurred.

6. Roles & Responsibilities

Every individual employed at McGill has a role to play in regards to effective risk management; however, the following roles are critical to the success of ERM:

Title	ERM Program Role
Board of Governors (BoG)	Governance and Policy Setting
Audit and Risk Committee	Reporting and Oversight (as delegated by BoG)
President and Vice-Chancellor	Executive Sponsorship
President's Executive Team (P7)	ERM Standing Committee
Vice-President (Administration and Finance)	ERM Administrative Oversight
Internal Audit Unit	ERM Facilitator

6.1 **Board of Governors:**

6.1.1 Approves risk management policies;

6.1.2 Encourages an open and receptive risk management culture; and,

6.1.3 Oversees risk management within the University (delegated to the Audit and Risk Committee).

6.2 **Audit and Risk Committee:**

6.2.1 Receives and reviews periodic reports on risk management, including the ERM program and its implementation; and,

6.2.2 Recommends to the Board modifications to the University ERM program and related policies and frameworks.

6.3 **President and Vice-Chancellor – Executive Sponsor:**

6.3.1 Ultimate Owner of ERM at McGill;

6.3.2 Inspires and fosters cultural change in support of ERM as a value and best practice;

6.3.3 Leads the setting of strategic objectives for the University; and

6.3.4 Leads management discussions with the Board regarding institutional strategy and risk philosophy.

6.4 **President's Executive Team (P7) – ERM Standing Committee:**

6.4.1 Formal identification of strategic risks that have an impact on the University's goals;

6.4.2 Determination of priorities and risk rankings;

6.4.3 Development of strategic risk management plans;

6.4.4 Delegation of risk management activities (as appropriate); and,

6.4.5 Monitoring progress in managing risk.

6.5 **Vice-President (Administration and Finance) - Administrative oversight of ERM**

6.5.1 Responsible and accountable for overseeing the development, implementation, and fostering of a collaborative, campus-wide approach to ERM at the University;

6.5.2 Oversees the University's processes for identifying, analyzing, evaluating, responding to and controlling, monitoring, and reporting on key risks;

6.5.3 Oversees reporting on risks to the Executive Team and Audit and Risk Committee; and,

6.5.4 Ensures appropriate staffing and budget is allocated to ERM.

6.6 **Internal Audit Unit – ERM Facilitator**

6.6.1 Facilitates development, oversight and maintenance of the ERM program;
6.6.2 Facilitates and coordinates the process of identifying, reviewing, and ranking the University's top risks;
6.6.3 Assigns, tracks, and monitors the University's top risks;
6.6.4 Facilitates action in those areas where improvements are required; and,
6.6.5 Reports the status of risks to the University's Executives and the Audit and Risk Committee.

AUTHORITY TO APPROVE PROCEDURES

7. The President and Vice-Chancellor, or her delegate, has the authority to establish and amend procedures necessary for the purpose of implementing this Policy.

REVIEW

8. This Policy will be reviewed by the Board of Governors at least once every five years following its adoption.