Enterprise Risk Management Framework

Department of Risk Management

Approval Authority: Board of Governors
Date of Original Framework: December 2, 2025

Carleton University

Purpose

The Enterprise Risk Management Program and Framework establish the University's structured approach to identifying, assessing, treating, monitoring, and reporting enterprise and operational risks. It supports risk-informed decision-making, aligns risk management with institutional strategy and governance, and promotes a risk-aware culture focused on accountability, transparency, continuous improvement, and the creation, preservation, and realization of value.

Scope

The Framework applies to members of the Board of Governors, faculty, staff, students, visitors, contractors, academic and administrative leaders, and all areas of the University responsible for identifying, evaluating, managing, monitoring, and reporting risks. Risk ownership rests with the individuals and units accountable for managing risks within their areas of responsibility, while the Department of Risk Management maintains responsibility for the Enterprise Risk Management Framework and related processes.

Background and Understanding

Enterprise Risk Management is a strategic and systematic approach used to identify, assess, manage, monitor, and report risks across the University. It supports a common understanding of uncertainty, potential impacts, opportunities, and mitigation requirements across academic, administrative, operational, financial, legal, compliance, technological, reputational, and strategic activities.

The Framework is adaptable to different institutional, portfolio, departmental, project, and program contexts. This flexibility allows risk management practices to be scaled to the nature, complexity, and significance of the activity while maintaining consistent principles, terminology, governance expectations, and reporting standards.

Program Objectives

The Framework supports University leadership in identifying sustainable academic, research, operational, and strategic opportunities; supporting decisions to proceed with or terminate activities; avoiding opportunities that expose the University to excessive risk; strengthening service delivery and accountability; improving administrative controls; supporting resourcing and workload decisions; and planning coordinated responses to emerging risks and risk events.

Program Benefits

- Provides awareness of, and responsiveness to, the University-wide risk landscape and horizon.
- Enhances the University's ability to monitor and comply with legal and regulatory requirements.
- Increases confidence that leadership can achieve strategic objectives and priorities.
- Improves portfolio risk management by identifying interconnected risks.
- Integrates risk management into day-to-day operations and planning.
- Enables consistent, risk-informed decision-making across the University.

Guiding Principle

The following principles guide Carleton University's approach to Enterprise Risk Management and support consistent, accountable, and risk-informed decision-making across the University:

- Risk management creates and protects value by contributing to the achievement of objectives and improving performance across the University.
- Key risks will be identified, assessed, monitored, and reported in a systematic and consistent manner, supported by appropriate key risk indicators and mitigation actions.
- Oversight of risk management rests with the Board of Governors, supported by the Audit and Risk Committee and the University's established governance structures.
- The President, Vice-Presidents, senior management, directors, managers, academic leaders, and risk owners are accountable for supporting and implementing effective risk management practices within their areas of responsibility.
- Risk management is integrated into strategic planning, operational planning, resource allocation, project management, governance reporting, and day-to-day decision-making.
- Risk-informed decision-making supports balanced consideration of threats, opportunities, legal and regulatory obligations, institutional priorities, and the University's approved risk appetite.
- Internal Audit monitors the effectiveness of risk management processes and provides independent assurance and recommendations to strengthen controls and mitigation practices.
- The Associate Vice-President, Department of Risk Management, advises governance and management groups on the Framework, supports consistent application of risk management processes, and monitors and reports on the ERM Program.
- The ERM Program will be reviewed and improved on an ongoing basis to remain responsive to changes in the University's internal and external risk environment.

Vision and Risk Management Commitment

The University is committed to being a bold, dynamic, and innovative leader in higher education, providing an accessible, adaptable, and challenging learning environment that develops graduates and research responsive to regional, national, and international communities.

The Enterprise Risk Management Program supports this vision by creating a risk-aware culture that promotes principled decision-making through the identification, analysis, mitigation, and monitoring of risk.

Definitions

- **Risk:** The effect of an event or activity on the University's strategic or operational goals, expressed through the combination of impact and likelihood.
- **Risk Management Process:** Coordinated activities used to direct and control the University with respect to risk. The process establishes context, identifies, analyzes, evaluates, treats, monitors, reviews, communicates, and reports risk.
- **Risk Committee:** A senior management committee responsible for supporting the analysis, evaluation, prioritization, and oversight of key enterprise risks facing the University.
- **Inherent Risk:** The level of risk that exists in the absence of actions, controls, or mitigation measures that management may take to alter the likelihood or impact of the risk.
- **Residual Risk:** The level of risk remaining after risk treatment, controls, or mitigation measures have been applied.
- **Enterprise Risk Management:** A systematic and integrated approach to managing uncertainties that may affect the University's strategic objectives and ability to create, preserve, and realize value.
- **Operational Risk Management:** A systematic approach to managing uncertainties arising from inadequate or failed internal processes, people, systems, external events, or operational activities. Operational risk management is practiced at the department, faculty, project, program, or unit level and provides important input into Enterprise Risk Management.

- **Risk Management Framework:** A set of components that provides the foundation and organizational structure for designing, implementing, monitoring, reviewing, communicating, and continually improving risk management across an organization.
- **Enterprise Risk Management Framework:** The University's institution-wide framework for applying risk management principles, governance, accountability, reporting, and continuous improvement to enterprise and operational risks.
- **Risk Appetite:** The types and amount of risk the University is willing to accept in pursuit of its strategic objectives.
- **Risk Owner:** An individual with responsibility, accountability, and authority to manage a risk and prepare mitigation plans.
- **Risk Treatment:** The process of modifying risk through acceptance, avoidance, transfer, reduction, or exploitation of opportunity.
- **Key Risk Indicator:** A measure that indicates the potential presence, level, or trend of a risk.

Enterprise Risk Management Framework

The Enterprise Risk Management Framework provides the foundation and organizational structure for designing, implementing, monitoring, reviewing, communicating, and continually improving risk management across the University. It supports a consistent, integrated, and scalable approach to managing uncertainty, enabling the University to identify risks and opportunities, assess their significance, assign accountability, implement appropriate treatment strategies, and report material risk information through established governance channels.

The Framework is intended to be applied at both the enterprise and operational levels. At the enterprise level, it supports the identification and oversight of risks that may affect institutional strategy, reputation, compliance, financial sustainability, safety, continuity, and long-term objectives. At the operational level, it provides a common approach for departments, faculties, projects, and programs to identify, assess, treat, monitor, and report risks within their areas of responsibility.

- **Principles:** Establish a risk-aware culture that creates and protects value, supports due diligence, promotes informed decision-making, encourages appropriate risk-taking, and reinforces legal, regulatory, and policy compliance as a minimum standard.
- **Risk assessment:** Provide common methods for identifying risks, assessing likelihood and impact, assigning risk scores, evaluating risk against appetite, and prioritizing mitigation.
- **Governance and accountability:** Define roles, responsibilities, oversight expectations, reporting relationships, and escalation pathways for the Board, Audit and Risk Committee, senior management, risk owners, Internal Audit, and the Department of Risk Management.

- **Risk treatment and mitigation:** Support the development of mitigation plans, treatment options, assigned responsibilities, timelines, resources, monitoring measures, and reassessment of residual risk.
- **Monitoring and reporting:** Establish expectations for ongoing review, risk reporting, key risk indicators, stakeholder communication, governance updates, and continuous improvement.

The Framework also informs internal audit planning by helping identify operational areas where assurance may be required. It is designed to align with recognized risk management practices, including International Organization for Standardization (ISO) 31000 principles, while remaining adaptable to Carleton's institutional context, strategic priorities, and evolving risk environment.

Enterprise Risk Management Process

The Enterprise Risk Management process is a cyclical approach used to identify, assess, manage, monitor, and report risks that may affect the University's strategic and operational objectives. The cycle supports consistent decision-making, strengthens accountability, and ensures that risk information is reviewed and updated as circumstances change. The process is intended to be adaptive, evidence-informed, and integrated with institutional planning, governance, and reporting practices.

- **Set objectives and establish context:** Define objectives, align ERM with institutional priorities and strategy, identify internal and external factors, and consider risk appetite when establishing the scope and criteria for assessment.
- **Risk identification:** Identify and catalogue potential risks across the University, including both internal and external risks that could affect strategic priorities, operations, compliance, reputation, finances, technology, health and safety, or service delivery.
- **Risk ownership:** Assign clear accountability for each risk by identifying risk owners and defining roles, responsibilities, and expectations for managing outcomes.
- **Risk assessment and analysis:** Evaluate the likelihood and impact of each risk, consider relevant attributes and key risk indicators, and prioritize risks based on their significance to institutional objectives.
- **Risk evaluation:** Compare assessed risks against the University's risk appetite, taking into account existing mitigation, legal or policy requirements, cost-benefit considerations, and institutional context.
- **Risk treatment:** Develop and implement appropriate strategies to avoid, reduce, transfer, accept, or exploit risks, supported by mitigation plans, timelines, assigned responsibilities, and monitoring expectations.
- **Monitoring and reporting**: Continuously monitor risks, controls, mitigation progress, and emerging trends, and report material risk information through established governance and management channels.

- **Communication and consultation**: Engage stakeholders throughout the process to ensure risk information is timely, meaningful, consistent, and aligned with decision-making needs.
- **Review, monitor, and improve:** Use audits, benchmarking, governance feedback, stakeholder input, incident learning, and maturity reviews to continually improve the ERM Program and Framework.

Outputs from the ERM process – including risk assessments, audit findings, benchmarking, key risk indicators, stakeholder feedback, governance reporting, incident learning, and mitigation updates – are used as results and data inputs to strengthen awareness, support consultation, inform decision-making, and drive continual improvement of the ERM Program and Framework.

Risk Appetite

Risk appetite defines the level and types of risk the University is willing to accept in pursuit of its strategic objectives. The Board of Governors, senior management, and staff will consider the University's risk appetite in strategic and operational decisions. While the University generally maintains a limited risk appetite, it recognizes that some activities – particularly those that advance innovation, research, leadership in higher education, and long-term sustainability – may involve greater uncertainty. Risk appetite may therefore vary between the institutional level and the activity level, provided that decisions are made with a clear understanding of potential benefits, consequences, safeguards, and accountabilities.

In applying risk appetite, the University seeks to uphold ethical governance and responsible stewardship, support innovation without unnecessary bureaucracy, and avoid a risk-averse culture that suppresses growth or opportunity. The University prioritizes minimizing legal, operational, compliance, health and safety, and people-related risks, while accepting certain levels of uncertainty where doing so supports approved strategic objectives and where appropriate mitigation measures are in place. In some circumstances, inaction may create greater institutional risk than carefully managed action.

Approval of the University's risk appetite rests with the Board of Governors. Implementation is the responsibility of the University's executive leaders, Deans, Associate Vice-Presidents, Assistant Vice-Presidents, Chairs, Directors, Managers, and risk owners within their respective areas of accountability.

Risk Appetite Categories

The University's risk appetite is expressed through three broad categories: Conservative, Balanced, and Entrepreneurial. These categories guide the degree of uncertainty the University may accept and support consistent, transparent decision-making across portfolios and activities.

Level of Risk Appetite	Risk Approach	Tolerance	Options
Entrepreneurial	The university is willing to take calculated risks in pursuit of strategic opportunities that advance its mission, innovation or financial sustainability.	Willing to accept a reasonable degree of uncertainty or variability.	The university will select the most advantageous option while accepting the possibility of failure to achieve objectives.
Balanced	The university is willing to adopt a measured and proportionate approach to risk-taking while maintaining safeguards.	Willing to accept limited changes or alterations from plan.	The university will select the option that presents limited risk to strategic priorities while providing benefits.
Conservative	The university is willing to take a cautious and risk-averse approach prioritizing preservation of assets, compliance and reputation.	Willing to accept only a very limited deviation from existing plans, policy, procedures and processes.	The university will select the option with little likelihood of failure to achieve objectives.

Risk Categories

The Framework uses a comprehensive risk classification approach to capture the full range of potential exposures facing the University. Risk categories support consistent identification, assessment, reporting, and monitoring of material risks and help ensure that strategic, emerging, operational, and financial risks are considered through a common enterprise lens.

- **Strategic risks:** Risks and uncertainties that affect the University's strategy, strategic priorities, long-term objectives, reputation, financial sustainability, or ability to execute its mission. These risks generally have enterprise-wide implications and require coordinated planning, governance oversight, and mitigation.
- **Emerging risks:** New, evolving, or difficult-to-predict risks that may arise from changes in the internal or external environment, including technological change, regulatory shifts, climate-related pressures, sector disruption, demographic trends, or other developing conditions. These risks may not yet be fully understood or quantified but may have significant future impact.

- **Operational risks:** Risks arising from internal processes, people, systems, services, facilities, technology, health and safety, compliance activities, or day-to-day operations. Operational risks may affect service delivery, financial stability, continuity, safety, compliance, and reputation, and may serve as important inputs into the enterprise risk reporting cycle.
- **Financial risks:** Risks related to losses, cost overruns, funding shortfalls, budget pressures, revenue volatility, unexpected liabilities, insurance exposures, or other financial events that may materially affect the University's ability to meet strategic objectives, sustain operations, preserve assets, or maintain long-term financial stability.
- **Technology-related risks:** may include cybersecurity, privacy, data governance, system resilience, information integrity, access management, and the availability and reliability of critical systems and digital services.

Risk Identification and Stakeholder Engagement

As an integral part of the University's Enterprise Risk Management cycle, the Department of Risk Management engages with a diverse group of stakeholders to support risk identification, analysis, and prioritization. Stakeholders may include internal participants such as academic and administrative staff, as well as external parties such as other higher-education institutions, auditors, consultants, insurers, and other relevant advisors. These interactions provide valuable insight into events, trends, opportunities, and emerging issues that may affect the University's objectives.

When identifying major risks, the University must consistently assess potential impacts. Risks may affect institutional strategic objectives differently than they affect individual projects, departments, faculties, or programs. Decisions at all levels should therefore consider enterprise-level impact in relation to the University's goals, priorities, obligations, and risk appetite.

- **Activities and impact:** Stakeholders provide perspectives on events, activities, or conditions that may lead to loss, disruption, non-compliance, reputational harm, or other adverse impacts on the University's goals and objectives. Understanding these risks from multiple viewpoints helps the risk team prioritize mitigation efforts effectively.
- **Opportunities:** Stakeholders identify areas where risk management practices may enhance performance, support strategic priorities, or improve decision-making. These insights help align risk management activities with institutional objectives and the responsible pursuit of opportunity. Opportunities will be evaluated using the opportunity matrix within the enterprise risk management software to support consistent assessment, prioritization, and documentation.

- **Emerging risks:** Stakeholders contribute insight into new, evolving, or uncertain threats that could affect the institution. This proactive engagement helps the University anticipate potential risks, adapt strategies, and remain responsive to changes in the internal and external environment.

Risk Owners

Identifying risk owners is integral to the success of the Enterprise Risk Management Program. Risk owners are accountable for managing specific risks throughout the risk lifecycle and are responsible for identifying, analyzing, monitoring, and addressing risks within their areas of responsibility. Their role is to ensure that appropriate risk mitigation strategies are developed, implemented, monitored, and updated as risk conditions change.

Each risk will be assigned to a risk owner who will be expected to:

- Ensure that approved mitigation plans are enacted.
- Resolve issues that may affect the successful implementation of mitigation actions.
- Monitor and provide status reports on risk mitigation plans to the Associate Vice-President, Department of Risk Management.
- Collaborate with the Department of Risk Management and Risk Steering Committee members by sharing relevant risk information, mitigation plans, progress updates, and emerging issues.
- Review and update mitigation plans as risks mature or as likelihood, impact, controls, or operating conditions change.

Risk Assessment and Evaluation

Risk assessment and evaluation provide a consistent method for understanding the significance of identified risks and prioritizing management attention. The process considers the likelihood of a risk occurring and the potential impact on the University's strategic and operational objectives. Assessment may include both qualitative and quantitative information, professional judgment, scenario analysis, stakeholder input, and relevant key risk indicators.

Risk analysis enables the University to compare risks using a common scale, identify the most significant exposures, and focus mitigation efforts on the risks that could most materially affect institutional priorities, compliance obligations, financial sustainability, service delivery, safety, reputation, and continuity of operations.

Risk Rating Criteria – Impact

Impact of Risk	Strategic	Legal	Operational	Technological	Financial	Reputational
5 – Severe	Activity or event does not support any pillar in the Strategic Plan or other strategic planning documents or policies.	Potential for major litigation; termination of contracts; no indemnity to the University; criminal charges; or fines exceeding $10,000,000 for non-compliance.	Potential for internal or external fraud, injury to students or workers, damage to physical assets, business disruption, or significant changes to processes.	May require major change to enterprise IT systems involving multiple associated applications or significant upgrades to several faculty or department IT systems; may create a single point of failure for critical systems; requires collection of a large amount of personal data.	Greater than 5% impact to strategic mandate, business objective, multiple business objectives, or a business objective that also affects the strategic mandate.	May result in multiple reports from national, international, and social media outlets for longer than seven days.
4 – Significant	Activity or event supports one pillar in the Strategic Plan and one other planning document or policy.	Potential for numerous moderate litigation matters; possible default or increased assumption of risk under contract; no indemnity to the University; or fines exceeding $5,000,000 and orders under regulations.	Potential for injury to students or workers, damage to physical assets, business disruption, or changes to processes.	May require significant change to an enterprise IT system involving at least one associated application or several faculty or department IT systems; requires collection of a significant amount of personal data.	3.1% to 5% impact to strategic mandate, business objective, multiple business objectives, or a business objective that also affects the strategic mandate.	May result in multiple reports from national and social media outlets over a three- to seven-day period.
3 – Moderate	Activity or event supports two pillars in the Strategic Plan and two other planning documents or policies.	Potential for a single moderate litigation matter or numerous small litigation matters; limited contractual indemnity for the University but not completely reciprocal; or potential rescinding of licences required by regulations.	Potential impact to physical assets, business disruption, or changes to processes.	May require changes to several faculty or department IT systems; requires collection of data from several groups involving 2,000 records or less.	1.1% to 3.0% impact to strategic mandate, business objective, multiple business objectives, or a business objective that also affects the strategic mandate.	May result in multiple reports from regional media, where controlled, and social media outlets for three days or longer.

2 – Minor	Activity or event supports three pillars in the Strategic Plan and two other planning documents or policies.	Potential for a single minor litigation matter; reciprocal indemnity included in contract; or minimum compliance issues with regulations.	Potential for damage to physical assets or changes to processes.	May require changes to one faculty or department IT system; requires collection of data from one group of 1,000 records or less.	0.5% to 1.0% impact to strategic mandate, business objective, multiple business objectives, or a business objective that also affects the strategic mandate.	May result in minor coverage in local media or social media.
1 – None or Insignificant	Activity or event supports all four or more pillars in the Strategic Plan and any other planning documents or policies.	Potential for threat of litigation requiring small payout; indemnity clause fully in favour of the University; risk fully transferred; or exceeds compliance requirements and regulations.	Potential for changes to processes only.	Does not require IT system changes; no collection of personal data.	Less than 0.5% impact to strategic mandate, business objective, multiple business objectives, or a business objective that also affects the strategic mandate.	No mention in news media or social media.

Risk Rating Criteria – Likelihood

Likelihood Rating	Frequency	Description
5	Almost Certain	Quite probable that the risk will occur.
4	Likely	More likely than not that the risk will occur in the next 36 months.
3	Possible	Somewhat likely that the risk will occur in the next 36 months.
2	Unlikely	Low possibility that the risk will occur in the next 36 months.
1	No Chance or Rare	Very low possibility that the risk will occur in the next 36 months.

Risk Evaluation

Risk evaluation involves determining the acceptability of assessed risks in relation to the University's risk appetite. Consideration should be given to existing mitigation, the cost and benefit of further treatment, applicable policy or legal requirements, available resources, and other factors within the University's operating context.

Impact and likelihood are combined to generate a risk score. The resulting score is used to compare and prioritize risks, support escalation decisions, and focus resources on the risks that require the greatest management attention. Risk scores also support consistent reporting

through the Enterprise Risk Report, risk registers, heat maps, mitigation updates, and governance reporting.

- **Impact:** Impact reflects the potential consequence of a risk event on the University. Impacts may be assessed across strategic, legal, operational, technological, financial, reputational, health and safety, compliance, and service delivery dimensions.
- **Likelihood:** Likelihood reflects the probability or frequency of a risk occurring within the assessment period. The Framework uses a five-point scale ranging from rare or very unlikely through to almost certain.
- **Risk score:** The risk score is calculated by combining the assessed impact and likelihood of the risk. This score supports relative prioritization and helps identify whether the risk is low, moderate, high, or critical.
- **Risk evaluation:** Assessed risks are compared against the University's risk appetite, existing controls, legal and policy obligations, available resources, mitigation costs, and the broader institutional context.

Risk Score	Risk Level	Description
1-4	Low	Manage by routine procedures; should not require much attention but should be reviewed at least every 18 months.
5-10	Moderate	Manage by specific monitoring or response procedures; should be monitored and reviewed every 12 months.
11-18	High	Requires escalation to Vice-President; should be constantly monitored and reviewed every three months. Risks and mitigation will be reported to the Audit and Risk Committee through the Enterprise Risk Report every six months.
19-25	Critical	Requires escalation to Audit and Risk Committee through the Enterprise Risk Report with mitigations reported. University management ensures risk is constantly monitored while undertaking regular risk mitigation activities.

***** Please note that for any identified Critical risks, senior management will consult with the Audit & Risk Committee regarding increased reporting frequency.**

Likelihood

Impact	No Chance 1	Unlikely 2	Possible 3	Likely 4	Almost Certain 5
SEVERE 5	Moderate (5)	Moderate (10)	High (15)	Critical (20)	Critical (25)
SIGNIFICANT 4	Low (4)	Moderate (8)	High (12)	High (16)	Critical (20)
MODERATE 3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Low 2	Low (2)	Low (4)	Moderate (6)	Moderate (8)	Moderate (10)
NONE or INSIGNIFICANT 1	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

Impact x Likelihood = Risk Score

Risk Treatment and Mitigation

Risk treatment involves selecting and implementing one or more strategies to modify a risk after it has been assessed and evaluated. Treatment decisions should be informed by the University's risk appetite, the level of residual risk, existing controls, regulatory or policy obligations, available resources, cost-benefit considerations, and the potential impact on institutional objectives. Multiple treatment strategies may be used for a single risk where doing so provides a more effective and proportionate response.

- **Avoidance:** Removing the risk source or discontinuing an activity, process, program, or decision that creates unacceptable risk exposure.
- **Reduction:** Implementing controls, actions, or safeguards to reduce the likelihood, impact, or overall exposure associated with the risk.
- **Transfer:** Sharing or transferring part of the risk to another party through mechanisms such as insurance, contracts, indemnities, outsourcing, or other risk-sharing arrangements.
- **Acceptance:** Retaining the risk by informed decision where the risk is within appetite, further treatment is not proportionate, or the risk is accepted to support a strategic opportunity.
- **Exploitation:** Applying additional resources or actions to realize value where a risk presents a positive opportunity aligned with the University's goals.

Risk mitigation plans establish accountability and help ensure that risk management responsibilities are assigned, actioned, monitored, and reported. Mitigation plans should identify the risk owner, required actions, timelines, resource requirements, escalation expectations, monitoring measures, and reporting obligations. Senior leadership is responsible for:

- Allocating risk mitigation responsibilities.
- Approving or assigning resources required to implement mitigation actions.
- Establishing timelines and milestones for completion.
- Measuring the presence, level, and trend of risks over time.
- Ensuring progress, actions, and target dates are reported to the Associate Vice-President, Department of Risk Management, as appropriate.
- Requiring escalation where risk exposure, mitigation delays, resource constraints, or residual risk levels warrant additional management or governance attention.

Following implementation of mitigation actions, the risk's likelihood, impact, and residual rating should be reassessed to determine whether the treatment has reduced the risk to an acceptable level and whether further action, monitoring, or escalation is required.

Monitoring, Review, and Continuous Improvement

Monitoring and review are planned and ongoing components of the Enterprise Risk Management process. They help confirm whether controls are effective and efficient in both design and operation, whether mitigation strategies remain appropriate, and whether changes in the University's internal or external environment require updated risk treatment, escalation, or reporting. Monitoring also supports the identification of emerging risks and enables the University to learn from events, trends, successes, failures, audit findings, benchmarking, and stakeholder feedback. Activities include:

- Reviewing operational activity reports and risk-related data from departments and portfolios.
- Assessing feedback from regulators, auditors, insurers, consultants, peer institutions, and other external stakeholders.
- Considering input from the Audit and Risk Committee, senior executive, faculty, staff, and other internal stakeholders.
- Monitoring changes in strategic priorities, regulatory expectations, operating conditions, external trends, and institutional risk criteria.
- Learning from incidents, near misses, audits, reviews, exercises, and other events that may indicate changes in exposure or control effectiveness.
- Conducting formal periodic review of the ERM Program and Framework using recognized standards, maturity models, benchmarking, and governance feedback.

Communication, Consultation, Recording, and Reporting

As part of a strong governance framework and to support effective risk management at Carleton University, timely and meaningful communication, consultation, recording, and reporting of risk information are critical. These activities support decision-making, strengthen accountability, and help ensure that risks are managed in line with the Enterprise Risk Management Framework.

Communication and consultation occur throughout the risk management lifecycle and involve the Board of Governors, Audit and Risk Committee, senior management, risk owners, faculty, staff, and other relevant stakeholders. Risk information should be concise, unambiguous, standardized, consistent, and integrated with existing planning, governance, and management reporting processes.

Reporting should provide users with the information required to understand key risks, risk levels, mitigation progress, emerging issues, and any required escalation.

User Group	Risk Information Needs	Typical Report Types	Timing
Board of Governors	Enterprise risk oversight, key enterprise risks, material changes, and mitigation progress.	Enterprise Risk Report, Key Enterprise Risk Register, and updates on mitigation.	At least annually, with mitigation updates generally every six months.
Audit and Risk Committee	Detailed oversight of enterprise risk exposures, risk trends, mitigation status, heat maps, and escalation items.	Enterprise Risk Report, Enterprise Risk Heat Map, Enterprise Risk Register, and mitigation updates.	At least annually, with mitigation updates generally every six months or more frequently for critical risks.
Senior Management	Portfolio and institutional risk information to support planning, resource allocation, prioritization, and risk-informed decisions.	All relevant risk reports, dashboards, registers, and mitigation updates.	Quarterly or as required.
Risk Owners	Detailed information on risks under their responsibility, including mitigation actions, timelines, controls, and reporting requirements.	Risk registers, mitigation plans, action tracking, status updates, and key risk indicators.	As required based on risk level and mitigation status.

Governance, Roles, and Responsibilities

Risk management is a shared responsibility across the University and is embedded within the University's governance, management, planning, and accountability structures. The governance model aligns risk oversight with decision-making at the Board, executive, portfolio, and operational levels, supporting transparency, clear roles and responsibilities, consistent reporting, and a strong risk-aware culture.

Governance Value Model

The governance value model emphasizes the alignment of risk management with the University's governance structure to support strategic objectives and enhance accountability. It integrates risk oversight into decision-making at all levels, particularly at the Board and executive levels, by promoting transparency, clear roles and responsibilities, and consistent reporting.

This model ensures that risk is not managed in isolation, but as part of the institution's broader commitment to ethical conduct, performance, and long-term value creation.

- **Board of Governors:** Provides oversight of the Enterprise Risk Management Program, approves the Enterprise Risk Management Policy and Framework, oversees key enterprise risks, and ensures that risk management supports the University's fiduciary, strategic, and governance responsibilities.
- **Audit and Risk Committee:** Supports the Board in overseeing enterprise risk management, reviewing the Enterprise Risk Report, risk appetite statements, enterprise risk registers, risk heat maps, internal audit observations, and mitigation progress.
- **President:** Provides general risk management oversight, promotes adoption of Enterprise Risk Management throughout the University, assesses top risks and action plans, reviews or approves major treatment options, and reinforces a strong risk management culture.
- **Vice-Presidents:** Are accountable to the President for risk management within their areas of responsibility, including identifying and managing enterprise and operational risks, implementing risk management policies and procedures, acting on audit and governance recommendations, and providing timely updates on risk status and treatments.
- **Associate Vice-President, Department of Risk Management:** Leads the development and implementation of the Enterprise Risk Management Framework and related policies, supports identification and prioritization of risks and opportunities, monitors mitigation progress, maintains the ERM plan and risk register, provides training and guidance, produces risk reports, and supports risk financing through insurance and related processes.
- **Internal Audit:** Monitors the effectiveness of the risk management framework, supports risk identification by assessing internal controls, recommends improvements to controls and mitigation practices, and periodically reviews ERM maturity.
- **Directors, managers, and academic leaders:** Incorporate risk management into standard management practices by identifying, assessing, treating, and reporting operational, emerging, and residual risks within their areas of responsibility.
- **Risk owners:** Maintain accountability for assigned risks, ensure mitigation plans are implemented, resolve issues affecting successful implementation, monitor and report on

mitigation progress, and collaborate with the Department of Risk Management and governance bodies as required.

- **Faculty, staff, students, visitors, and contractors:** Share responsibility for identifying, communicating, and managing risks in accordance with University policies, procedures, and applicable legal and regulatory requirements.

Review Cycle

The Enterprise Risk Management Policy and Framework will be reviewed on a regular cycle to ensure it remains current, effective, aligned with institutional priorities, and responsive to changes in the University's internal and external risk environment. The Framework is subject to formal review at least every five years, with the next mandatory revision scheduled for December 2030, or earlier if significant changes in governance, legislation, regulation, strategy, operations, risk appetite, or recognized risk management standards require an update.

Interim updates may be made where necessary to address emerging risks, audit findings, stakeholder feedback, changes in reporting requirements, lessons learned from incidents or exercises, benchmarking results, or maturity assessment findings. The Department of Risk Management is responsible for monitoring the continuing relevance of the Framework and coordinating updates, consultation, and reporting through the appropriate governance channels.

Approval of the Enterprise Risk Management Policy and Framework rests with the Board of Governors, supported by review and recommendation through the Audit and Risk Committee. Ongoing implementation, monitoring, and continuous improvement are supported by senior management, risk owners, Internal Audit, and the Department of Risk Management.