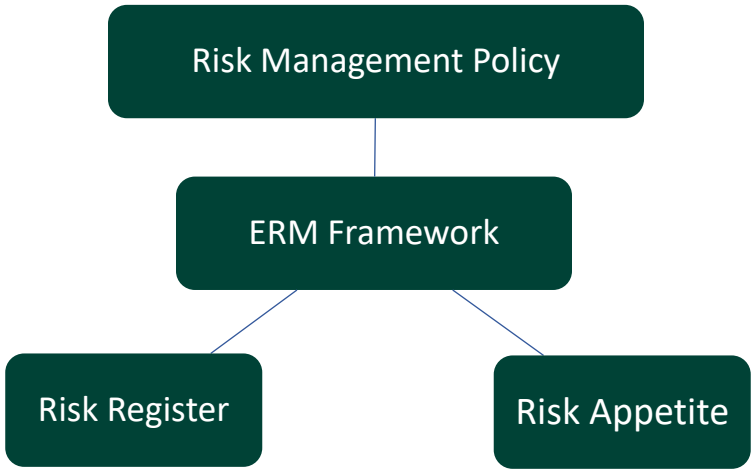
Procedure for Board Policy 1.4.9 – Enterprise Risk Management Framework

1. Overview

Enterprise Risk Management (ERM) – a continuous, proactive and dynamic process designed to identify, assess, communicate and manage potential risks; this includes negative risks that might otherwise inhibit King's from achieving its mission and strategic goals, as well as positive risks that align with King's goals and operational responsibilities.

2. ERM Program Structure

ERM documentation is structured and designed to guide the process and ensure King's can identify and prioritize the areas of highest risk and drive the appropriate mitigation actions. The ERM Program documentation follows the structure as outlined below.



2.1 Risk appetite refers to amount and type of risk that King's is willing to pursue or retain in the pursuit of value. It provides an important, forward-looking perspective and is a guide to risk management activities when determining how much risk is acceptable. King's will document and regularly review its risk appetite. Risk appetite reflects King's mission, vision, and values, and considers stakeholder expectations, and in turn, has an influence on both King's culture and operations.

2.2 King's will maintain a risk register of key strategic risks, indicators and other data derived from its ongoing ERM activities.

2.3 The Board is responsible for setting the "tone at the top" for institutional culture and supporting a culture that enables effective ERM. Clear expectations of conduct are fundamental to the ERM framework. They establish the institution's shared values and standards that guide core values, ethical behaviour, support sound decision-making, and mitigate legal, financial, operational, safety, and reputational risks. These expectations promote integrity and accountability by clarifying responsibilities and reinforcing compliance with applicable legislation, regulations, and institutional requirements. They also support a consistent approach to identifying, reporting, and addressing conduct-related concerns across the institution. Expectations of conduct apply across all ERM risk domains and must be consistent with applicable laws, collective agreements, and recognized professional ethical standards governing university, teaching, and professional practice including Guidelines concerning Professional Ethics and Professional Relationships of the Canadian Association of University Teachers, and the Guide to Proper Conduct of Research at King's. King's also has student, and board code of conducts. The alignment of values, risk appetite, and oversight shape a culture that underpins strong ERM.

2.4 The Board approved whistleblower policy is a key element of the ERM Framework, providing a safe, confidential, and non-retaliatory way to report suspected misconduct or policy violations. By enabling community members to speak up, it strengthens Kings' culture of integrity and supports early issue detection. Within the ERM framework, the program serves as an early-warning system. Reports help Kings identify emerging risks, address concerns before they escalate, and improve internal controls. This strengthens risk monitoring across financial, operational, compliance, safety, and reputational areas and supports more informed decision-making.

2.5 A central repository of tools will be maintained to enable the effective execution of the ERM Program. These documents will be regularly reviewed to identify improvement opportunities, ensuring they continue to consider the application of leading practices in King's specific context.

3. The Governance structure of the ERM Program is as below:

Board of Directors ***Chair: Chair, Board of Directors***
Audit *and Risk Management* Committee ***Chair: Chair, Audit and Risk Management Committee***

President's Executive Council *Chair: President*
Risk Management Steering Group ***Chair: President or Designate***

4. Roles

Specific roles related to the ERM Program are as follows:

4.1 The Board of Directors has ultimate accountability for risk and risk management.

4.2 The Audit and Risk Management Committee of the Board of Directors provides oversight of the ERM Program and monitors the management of key/top strategic-level enterprise risks. The Audit and Risk Management Committee will keep the broader Board of Directors informed of key developments, including any policy violations, and by responding to any new inquiries from the Board related to risk consistent with the committee's terms of reference.

4.3 The President's Executive Council provides leadership, commitment and assumes overall responsibility and accountability for ERM, and integration of associated processes into strategy. The President will present risk information on a regular basis (as outlined in paragraph 5.3 below) to the Audit and Risk Management Committee.

4.4 Appointed by the President, the Risk Management Steering Group is comprised of both academic and administrative units and coordinates all aspects of the assessment, treatment and monitoring of risks. These representatives act as a conduit of information to and from King's academic and administrative units, and will be tasked with the formulation of institution wide risks based on both 1) information from units and 2) their own assessment. The President or designate will act as the Chair of the Risk Management Steering Group, and will present risk information on a regular basis (as outlined in paragraph 6 below) to the President's Executive Council.

4.5 Internal control activities will support ERM by:

4.5.1 Providing assurance that the ERM Program and ERM process, including resulting internal controls, are effective; and,

4.5.2 Providing periodic reviews and reports on ERM to the Audit and Risk Management Committee of the Board.

5. Responsibilities

Specific responsibilities related to the ERM Program are as follows:

5.1 Board of Directors

5.1.1 Overall ownership and accountability for risk and risk culture

5.1.1.1 Setting the tone on risk assurance and identification, aligned with ethics, values and risk

5.1.2 Monitor compliance with the risk management processes

5.1.3 Review, approve and use Risk Appetite statements

5.1.4 Review status updates for key and emerging risks

5.1.5 Integrate risk into Board decisions

5.1.6 Approve the Whistleblower Policy

5.1.7 Approve Expectations of Conduct

5.2 Audit and Risk Management Committee of the Board of Directors

5.2.1 Oversight of the ERM process

5.2.2 Monitor the management of key/top strategic-level enterprise risks

5.2.3 Participate in the assessment of risks and development of mitigation strategies as required

5.2.4 Review status updates for key and emerging risks

5.2.5 Provide advice to the Board on risks to inform key decisions

5.2.6 Monitor emerging conditions or control weaknesses for key and emerging risks

5.2.7 Recommend a Whistleblower policy to the Board

5.2.8 Recommend Expectations of Conduct

5.3 President

5.3.1 Ensure the effective design, implementation, and maintenance of operational ERM practices

5.3.2 Ensure regular monitoring and reporting of risks, and report regularly to the Board through the Audit and Risk Management Committee

5.3.3 Recommend risk appetite to the Board, monitor and report regularly to the Board

5.3.4 Promote a risk-aware culture

5.3.5 Appoint a Chair of the Risk Management Steering Group and select members

5.3.6 Provide direction to the Risk Management Steering Group informed by the risk work of the President's Executive Council

5.3.7 Ensure the review of the strategic risks as provided by the Risk Management Steering Group

5.3.8 Draft Expectations of Conduct and revisions for Audit and Risk Management Committee consideration at an interval consistent with the board policy review cycle. Ensure code of conduct is implemented.

5.3.9 Facilitate reporting to the Audit and Risk Management Committee

5.4 President's Executive Council

5.4.1 Oversee the implementation and ongoing operation of the ERM Program and risk process

5.4.2 Establish and monitor risk appetite

5.4.3 Review risks assessed by the Risk Management Steering Group

5.4.4 Identify risks in addition to those provided by the Risk Management Steering Group

5.4.5 Oversee the development and execution of risk treatment strategies and mitigation projects

5.4.6 Assume responsibility ('ownership') for risks and controls within their areas of responsibility and validate/oversee treatment measures

5.4.9 Ensure ERM is linked to Strategic Priorities

5.4.10 Ensure appropriate resources and level of effort required to implement and operate ERM

5.5 Risk Management Steering Group

5.5.1 Identify, assess and monitor risks

5.5.2 Complete and maintain King's risk register

5.5.3 Execute risk mitigation strategies and projects as applicable

5.5.4 Provide guidance and training related to risk management activities as required

5.5.5 Facilitate action in those areas where improvements are required to the ERM process

5.5.6 Report regularly to the President's Executive Council

5.6 Chair of the Risk Management Steering Group

5.6.1 Lead the Risk Management Steering Group

5.6.2 Ensure the risk register is complete and maintained

5.6.3 Facilitate reporting to the President's Executive Council

5.6.4 Liaise with the President's Executive Council on a regular basis to ensure ERM Framework and process is functioning as intended

6. Internal Control

6.1 Internal Control activities support the ERM framework by providing independent assurance on the effectiveness of risk management, internal controls, and mitigation efforts. While risk ownership remains with administration, ERM data informs a risk-based internal control plan. Internal control activities also evaluate the ERM program's design, maturity, and effectiveness, offering objective assessments and guidance that strengthen risk governance and promote continuous improvement.

6.1.1 Proactively manage and mitigate risk

6.1.2 Ensure management use the appropriate tools and techniques to identify and perform risk analysis

6.1.3 Promote a common risk language and understanding of the negative and positive sides of risk

6.1.4 Leverage knowledge of King's and expertise in risk management and controls to champion ERM across King's

6.1.5 Act as the central point for driving organizational culture, and coordinating the assessment, monitoring and reporting of risks

6.1.6 Support management and risk committees as they make decisions on the best way to mitigate a risk

7. Reporting

Regular reporting is required to effectively monitor risks. King's will report its risk information as detailed in the table below.

Report Recipient	Type of Risk Management	Reporting Responsibility	Timing
Board of Directors	Status Update on ERM	Chair of Audit and Risk Management Committee	Annually
	Status Update for Key and Emerging Risks	Chair of Audit and Risk Management Committee	Annually
Audit and Risk Management Committee	Status Update for Key and Emerging Risks	President	Quarterly
	Risk Register	President	Annually
	Risk Appetite	President	Annually
President's Executive Council	Risk Register	Chair of Risk Management Steering Group	Annually
Risk Management Steering Group	Status Update for Key and Emerging Risks	Chair of Risk Management Steering Group	Quarterly

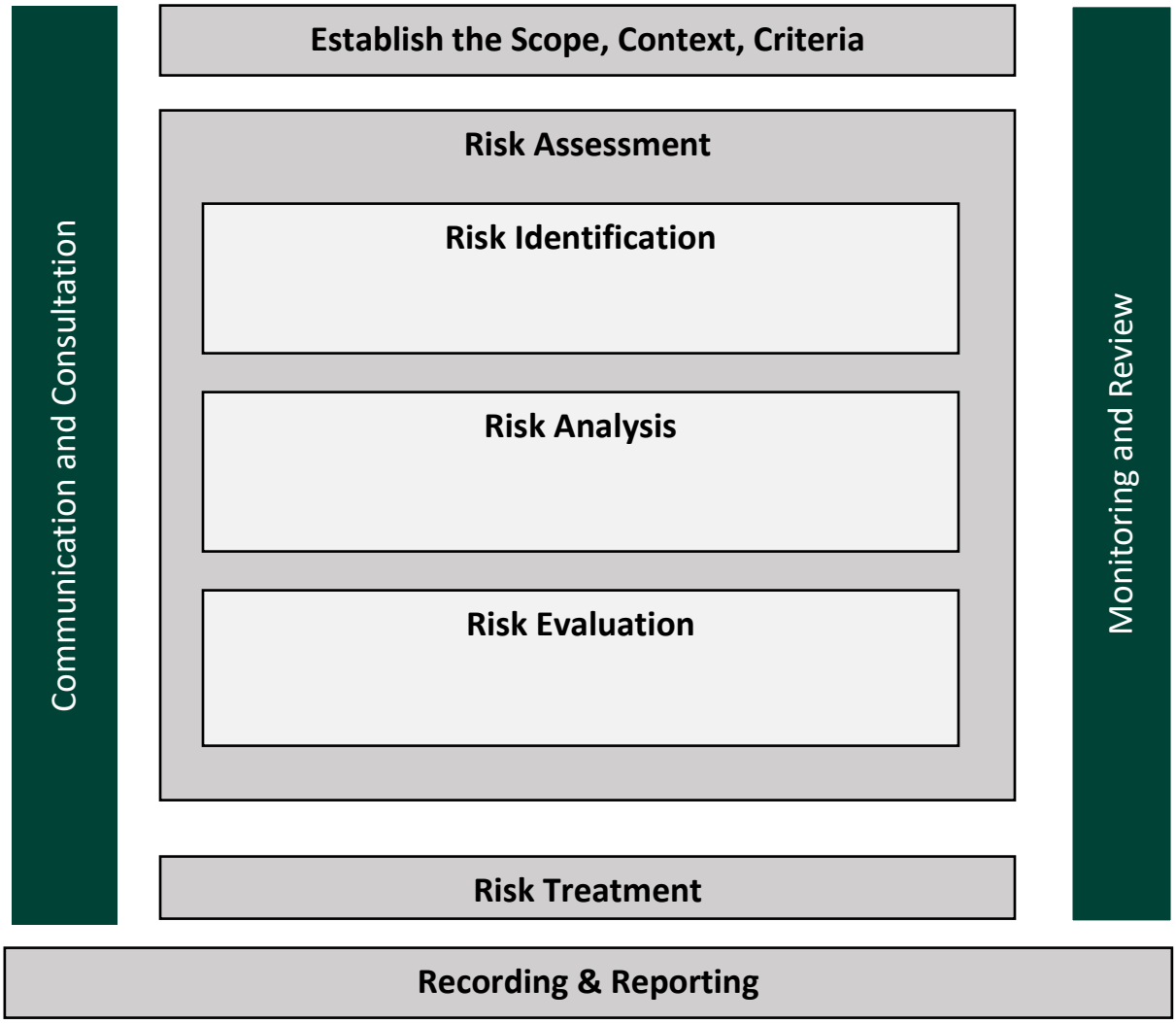
8. Training

Training is critical to the successful implementation and on-going operation of ERM at King's. To ensure all those with stated roles and responsibilities acquire and maintain the skills and knowledge needed for them to employ risk management activities, training will take place on ERM procedures, tools, roles, and responsibilities.

It is vital that individuals receive general training which covers all aspect of the ERM Program, as well as selective training commensurate with their roles and responsibilities. By way of example, it will be necessary for those on the Risk Management Steering Group to receive supplemental training and guidance on risk assessment, while those on the President's Executive Council receive additional training focused on risk governance and oversight.

9. ERM Process

Key to successful risk management is a structured process and approach. The process used by King's is based on ISO 31000:2018. It will be applied for institution wide risk management and can also be used for specific initiatives, projects or activities. The information below outlines the risk management steps.



Specific steps within the process are outlined below;

9.1 Communication and consultation with stakeholders is an integral part of the risk management process. Having a clear and effective governance structure, policy, reporting framework, and tools to convey risk assists with communication and consultation. King's will ensure effective communication and consultation are key components in the successful implementation of ERM as well as during the ongoing management of risk.

9.2 When establishing the context within its ERM process, King's will take into consideration the internal and external environments – as well as the purpose, goals, and objectives of the ERM Program, and the key internal and external interfaces/relationships that may impact the risk management process. Key considerations include any changes with respect to the expectations of stakeholders, policy requirements, strategic priorities and internal processes, policies, and procedures.

9.3 Risk Assessment: Consists of three main steps and will result in the understanding of the risk exposure present. The steps of a risk assessment are outlined below:

9.3.1 **Risk Identification:** As part of its ERM framework, Kings evaluates both sector-wide and institution-specific risks. Sector-wide risks reflect common regulatory, operational, financial, and reputational challenges in higher education, providing a baseline understanding of the environment. Institution-specific risks arise from Kings' unique mission, programs, governance, research, and strategic priorities, creating exposures or opportunities not shared by peer institutions. By considering both, the ERM program develops a comprehensive risk profile that supports informed decision-making, effective resource allocation, and proactive management of threats to Kings' mission, operations, and long-term sustainability. The process ensures that all potential risks are recognized, including those representing threats, opportunities, or both, and establishes a consistent, sustainable approach to risk identification. Risks related to artificial intelligence, cybersecurity, emerging technologies, as well as third-party risks will be considered as part of this broad assessment.

9.3.2 **Risk Analysis:** Risk analysis allows King's to consider the extent to which potential risks might have an impact on the achievement of strategic priorities. Such consideration is completed by following a standard and consistent approach to analyzing the likelihood or probability of the risk occurring, as well as its consequence or impact, should the risk occur. Once risks have been analyzed the information is documented in the risk register. King's will use the Probability-Consequence model of risk management.

9.3.3 **Risk Evaluation:** Once risks are identified and analyzed in accordance with the previous steps, the risk register is further developed. King's will use the risk register as the primary tool for articulating King's risk profile.

In evaluating risks for prioritization to drive further action, King's will take into account the degree of control King's has over each risk, the cost impact, benefits and opportunities presented by the risks. Where risk exceeds acceptability (i.e. risk appetite), additional risk treatment strategies and mitigating actions may be applied to reduce the level of risk. It should be noted that defining a risk as acceptable does not imply that the risk is insignificant. Reasons for deeming a risk to be acceptable at this stage include:

9.3.3.1 Probability and/or consequence of risk being so low that specific mitigation plans are not required

9.3.3.2 The risk being such that there are no mitigation actions available

9.3.3.3 Cost of mitigation plan is excessive as compared to the benefit such that acceptance of the risk is the only option

9.3.3.4 The risk is being driven by an external event/organization and therefore outside of the control of King's

9.3.4 **Risk Treatment:** Risk mitigation involves identifying the range of options or "controls" available for mitigating or "treating" risk and assessing the appropriateness of each alternative. Risk treatment refers to the policies, procedures, processes and other controls implemented to mitigate the probability and/or consequence of a risk. The President's Executive Council will oversee the development and execution of risk treatments. Once the optimal risk treatment is determined in the circumstance, King's will complete mitigation projects. It is not the intent in all cases to minimize, avoid or eliminate all risks that are identified, but more that King's understands the significant risks that may negatively impact King's and its strategic priorities. Such a balance is achieved by establishing a standard and consistent process for developing an acceptable risk treatment. Prior to selecting the appropriate risk treatment strategy, it is important to understand and identify the various risk treatment options available. Mitigation strategies can broadly be divided into the following four categories:

9.3.4.1 Avoidance – taking action to exit the activities that give rise to the risks 12.05.2 Reduction – reducing the risk probability, consequence, or both

9.3.4.2. Transfer – reducing risk probability or consequence by transferring or sharing a portion of the risk

9.3.4.3 Acceptance – taking no action to affect probability or consequence

9.3.5 **Monitoring & Review:** Regular monitoring and review of risks are essential to understanding the changing dynamic of risk. The President's Executive Council will monitor risks, provide updates to the Board of Directors and update the risk information as applicable with input from the Risk Management Steering Group.

9.3.6 **Recording & Reporting:** Throughout the process, the Risk Management Steering Group and the President's Executive Council will be recording information on individual risks as well as comprise reports on the greater inventory of risk information. There will be regular reporting between the groups, as well as to the Board of Directors.