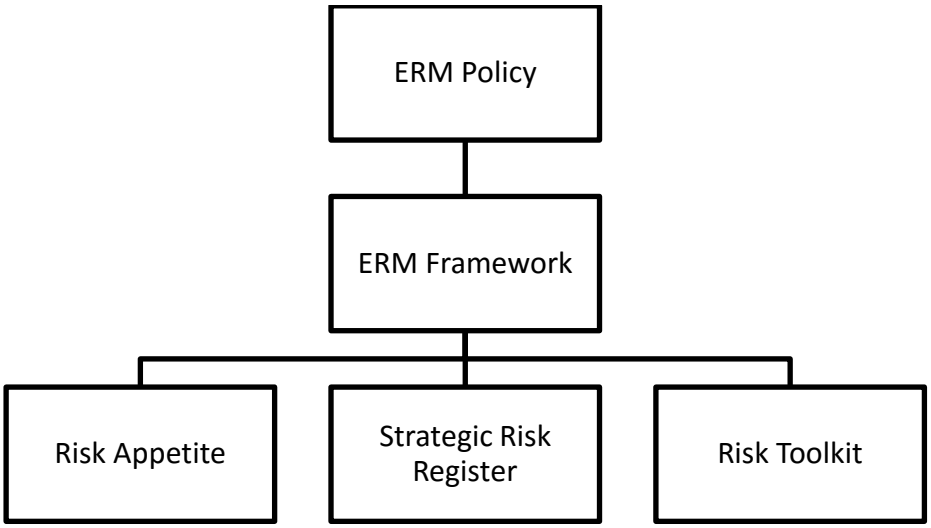
PROCEDURE FOR POLICY 1.55 – Enterprise Risk Management Framework

Overview

1.00 **Enterprise Risk Management –** a continuous, proactive and dynamic process designed to identify, assess, communicate and manage potential risks; this includes negative risks that might otherwise inhibit the University from achieving its strategic priorities and supporting objectives, as well as positive risks that are in alignment with the University's strategic priorities and operational responsibilities

ERM Program Structure

2.00 ERM documentation is structured and designed to guide the process and ensure Western 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.

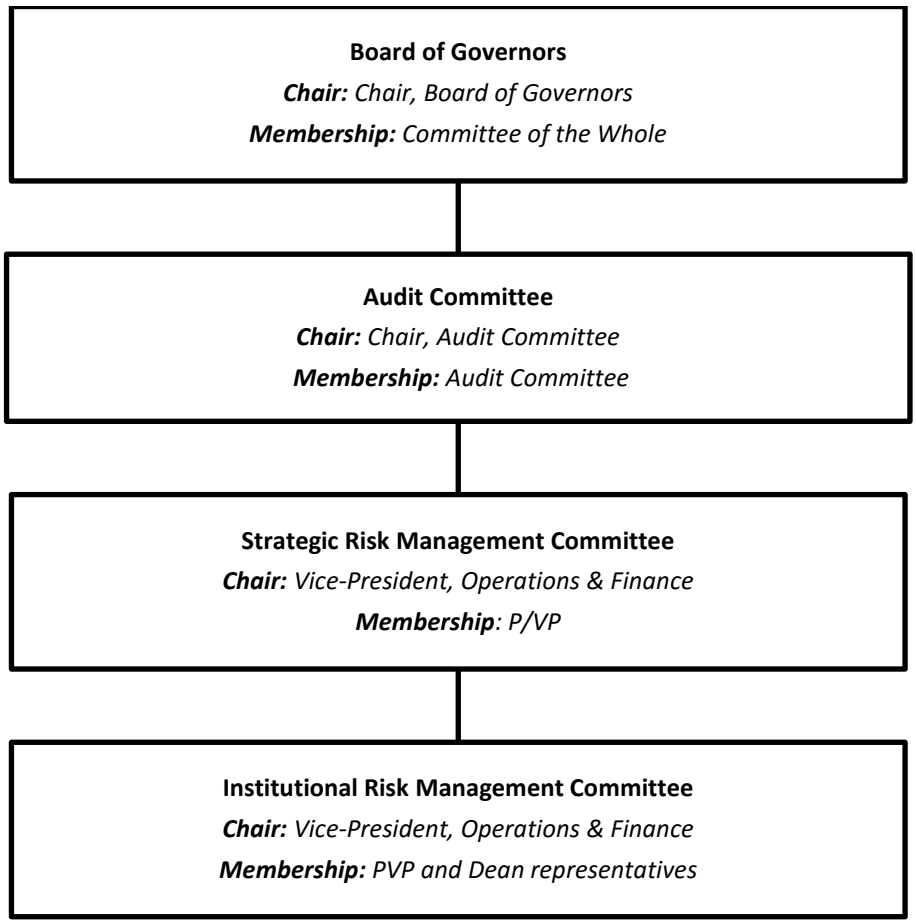


2.01 Risk appetite refers to amount and type of risk that an organization is willing to pursue or retain in the pursuit of value. It provides an important, forward-looking perspective and is a guide to risk management activities when determining how much risk is acceptable. Western will document and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

2.02 The University will maintain a formal register (the "Strategic Risk Register") of key strategic risks, indicators and other data derived from its ongoing ERM activities.

2.03 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 be in line with leading practice.

3.00 The Governance structure of the ERM Program is as below:



Roles

4.00 Specific roles related to the ERM Program are as follows:

4.01 The Board of Governors have ultimate accountability for risk and risk management.

4.02 The Audit Committee of the Board of Governors provides oversight of the ERM Program and monitors the management of key/top strategic-level enterprise risks. The Audit Committee will keep the broader Board of Governors abreast of key developments in the University's risks.

4.03 The Strategic Risk Management Committee provides leadership, commitment and assumes overall responsibility and accountability for ERM, and integration of associated processes into strategy. The Vice-President, Operations & Finance will act as the Chair of the Strategic Risk Management Committee and will present risk information on a regular basis (as outlined in paragraph 6 below) to the Audit Committee.

4.04 The Institutional Risk Management Committee is comprised of both academic and administrative areas and coordinates all aspects of the assessment, treatment and monitoring of risks. These representatives act as a conduit of information to and from all Western schools and departments, and will be tasked with the formulation of University-wide risks based on both 1) information from departments and 2) their own assessment. The

Vice-President, Operations & Finance will act as the Chair of the Institutional Risk Management Committee and will present risk information on a regular basis (as outlined in paragraph 6 below) to the Strategic Risk Management Committee.

4.05 In its regular course of duties, the Internal Audit Team will support ERM by:
- 4.05.1 Providing assurance that the ERM Program and ERM process, including resulting internal controls, are effective; and,
- 4.05.2 Providing periodic reviews and reports on ERM to the Audit Committee of the Board.

Responsibilities

5.00 Specific responsibilities related to the ERM Program are as follows:

5.01 Board of Governors
- 5.01.1 Overall ownership and accountability for risk
- 5.01.2 Monitor compliance with the risk management processes
- 5.01.3 Review, approve and utilize Risk Appetite statements
- 5.01.4 Review status updates for key risks
- 5.01.5 Integrate risk into Board decisions

5.02 Audit Committee of the Board of Governors
- 5.02.1 Oversight of the ERM process
- 5.02.2 Monitor the management of key/top strategic-level enterprise risks
- 5.02.3 Participate in the assessment of risks and development of mitigation strategies as required
- 5.02.4 Review status updates for key risks
- 5.02.5 Integrate risk into Board decisions
- 5.02.6 Monitor emerging conditions or control weaknesses for key risks

5.03 President
- 5.03.1 Ensure the effective design, implementation, and maintenance of ERM (policies and procedures)
- 5.03.2 Ensure regular monitoring and reporting of risks, and report regularly to the Board
- 5.03.3 Establish and monitor risk appetite, and report regularly to the Board
- 5.03.4 Promote a risk-aware culture

5.04 Strategic Risk Management Committee
- 5.04.1 Oversee the implementation and ongoing operation of the ERM Program and risk process
- 5.04.2 Establish and monitor risk appetite
- 5.04.3 Review risks assessed by the Institutional Risk Management Committee
- 5.04.4 Identify risks in addition to those provided by the Institutional Risk Management Committee
- 5.04.5 Oversee the development and execution of risk treatment strategies and mitigation projects
- 5.04.6 Assume responsibility (‘ownership’) for risks and controls within their areas of responsibility and validate/oversee treatment measures
- 5.04.7 Provide direction to the Institutional Risk Management Committee
- 5.04.8 Appoint a Chair of the Institutional Risk Management Committee and select members
- 5.04.9 Ensure ERM is linked to Strategic Priorities
- 5.04.10 Ensure appropriate resources and level of effort required to implement and operate ERM
- 5.04.11 Report regularly to the Audit Committee

5.05 Chair of the Strategic Risk Management Committee
- 5.05.1 Lead the Strategic Risk Management Committee
- 5.05.2 Ensure the review of the strategic risks as provided by the Institutional Risk Management Committee
- 5.05.3 Facilitate reporting to the Audit Committee

5.06 Institutional Risk Management Committee
- 5.06.1 Identify, assess and monitor risks
- 5.06.2 Complete and maintain the University-wide strategic risk register
- 5.06.3 Execute risk mitigation strategies and projects as applicable
- 5.06.4 Provide guidance and training related to risk management activities as required
- 5.06.5 Facilitate action in those areas where improvements are required to the ERM process
- 5.06.6 Report regularly to the Strategic Risk Management Committee

6.00 Chair of the Institutional Risk Management Committee
- 6.01 Lead the Institutional Risk Management Committee
- 6.02 Ensure the strategic risk register is complete and maintained
- 6.03 Sit as a member of the Strategic Risk Management Committee
- 6.04 Facilitate reporting to the Strategic Risk Management Committee
- 6.05 Liaise with the Strategic Risk Management Committee on a regular basis to ensure ERM Framework and process is functioning as intended

7.00 Internal Audit
- 7.01 Ensure management utilize the appropriate tools and techniques to identify and perform risk analysis
- 7.02 Promote a common risk language and understanding of the negative and positive sides of risk
- 7.03 Leverage knowledge of the University and expertise in risk management and controls to champion ERM across the University
- 7.04 Act as the central point for coordinating the assessment, monitoring and reporting of risks
- 7.05 Support management and risk committees as they make decisions on the best way to mitigate a risk

Reporting

8 Regular reporting is required to effectively monitor risks. The University will report its risk information as detailed in the table below.

Report Recipient	Type of Risk Management Information	Reporting Responsibility	Timing
Board of Governors	Status Update on ERM	Chair of Audit Committee	Annually
	Status Update for Key Risks	Chair of Audit Committee	Annually
Audit Committee	Status Update for Key Risks	Chair of Strategic Risk Management Committee	Semi-Annually
	Strategic Risk Register	Chair of Strategic Risk Management Committee	Annually
Strategic Risk	Strategic Risk Register	Chair of Institutional Risk	Annually

Management Committee		Management Committee	
	Status Update for Key Risks	Chair of Institutional Risk Management Committee	Quarterly

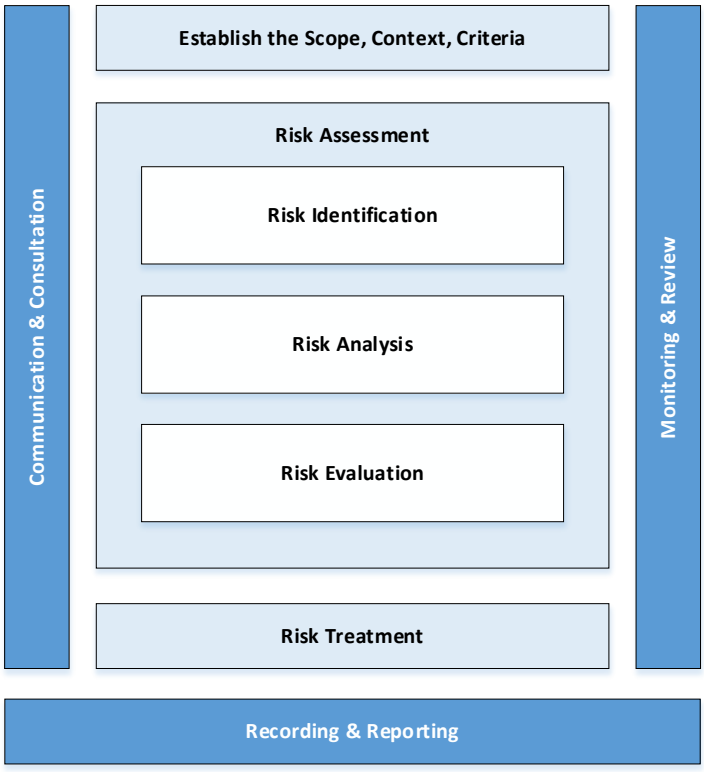
Training

9 Training is critical to the successful implementation and on-going operation of ERM at Western. 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.

10 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 Institutional Risk Management Committee to receive supplemental training and guidance on risk assessment, while those on Strategic Risk Management Committee receive additional training focused on risk governance and oversight.

ERM Process

11 Key to successful risk management is a structured process and approach. The process utilized by Western is based on ISO 31000:2018. It will be applied for University-wide risk management and can also be used for specific initiatives, projects or activities. The information below outlines the risk management steps. Supporting information and guidance on the process is found in the Risk Toolkit (specifically, refer to Appendix A - Risk Assessment Aide Memoire for a step-by-step guide for the completion of a risk assessment).



12 Specific steps within the process are outlined below; refer to Appendix A - Risk Assessment Aide Memoire for a step-by-step guide for the completion of a risk assessment:

12.02 **Communication & Consultation**: Communication and consultation with stakeholders is an integral part of the risk management process for Western and all organizations. Having a clear and effective governance structure, policy, reporting framework, and tools to convey risk assists with communication and consultation. Western will ensure effective communication and consultation are key components in the successful implementation of ERM as well as during the ongoing management of risk.

12.03 **Establish the Scope, Context, Criteria:** When establishing the context within its ERM process, Western 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.

12.04 **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:

12.04.1 **Risk Identification**: This step of the risk management process involves the identification of risks which arise from the external environment as well as from internal sources. As unidentified risks can pose a major threat to the achievement of strategic priorities and goals, it is important to ensure that the full range of risks is identified, including distinguishing between events that represent risks, those representing opportunities, and those that may be both. The objective of risk identification step is to develop a consistent and sustainable approach to identify risks.

12.04.2 **Risk Analysis**: Risk analysis allows the University 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 a Strategic Risk Register. Western will utilize the Probability-Consequence model of risk management.

12.04.3 **Risk Evaluation**: Once risks are identified and analyzed in accordance with the previous steps, a Strategic Risk Register is further developed. The University will use a Strategic Risk Register as the primary tool for articulating Western's risk profile.

In evaluating risks for prioritization to drive further action, Western will take into account the degree of control the University 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:

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

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

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

12.04.3.4 The risk is being driven by an external event/organization and therefore outside of the control of the University

12.05 **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 Strategic Risk Management Committee will oversee the development and execution of risk treatments. Once the optimal risk treatment is determined in the circumstance, the University 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 Western understand the significant risks that may negatively impact the University and the stated 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:

12.05.1 ***Avoidance*** – taking action to exit the activities that give rise to the risks

12.05.2 ***Reduction*** – reducing the risk probability, consequence, or both

12.05.3 ***Transfer*** – reducing risk probability or consequence by transferring or sharing a portion of the risk

12.05.4 ***Acceptance*** – taking no action to affect probability or consequence

12.06 **Monitoring & Review**: Regular monitoring and review of risks are essential to understanding the changing dynamic of risk. The Strategic Risk Management Committee will monitor risks, provide updates to the Board of Governors and update the risk information as applicable with input from the Institutional Risk Management Committee.

12.07 **Recording & Reporting**: Throughout the process, the Institutional Risk Management Committee and the Strategic Risk Management Committee 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 Governors. Templates for reports can be found in the Risk Toolkit.

GLOSSARY

C

Communication and consultation – continual and iterative processes that an organization conducts to provide, share or obtain information and engage in dialogue with stakeholders regarding the management risk

Consequence – outcome of an event affecting objectives

Control – measures that maintains and/or modifies risk

E

Establishing the context – defining the external and internal parameters to be taken into account when managing risk, and setting the of risk criteria

Event – occurrence or change of a particular set of circumstances

External context – external environment in which the organization seeks to achieve its objectives

I

Internal context – internal environment in which the organization seeks to achieve its objectives

L

Level of risk – magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

Likelihood – chance of something happening

M

Monitoring – continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

R

Risk – effect of uncertainty on objectives, deviation from the expected (positive and/or negative)

Risk analysis – process to comprehend the nature of risk and to determine the level of risk

Risk appetite – the amount of risk, on a broad level, an entity is willing to accept in pursuit of value

Risk assessment – overall process of risk identification, risk analysis and risk evaluation

Risk criteria – terms of reference against which the significance of a risk is evaluated

Risk evaluation – process of reviewing result of risk analysis to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk identification – process of finding, recognizing and describing risks

Risk owner – person or entity with the accountability and authority to manage a risk

Risk profile – description of any set of risks; the set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined

Risk source – elements which alone or in combination has the potential to give risk to risk

Risk treatment – process to modify risk

S

Stakeholder – person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity