



# Board of Governors Policy

**POLICY TYPE:** Enterprise Risk Management                      **NUMBER:** GP-7

**POLICY TITLE:** Governance Principles

**EFFECTIVE DATE:** November 10, 2021                      **REVISION DATE:** NEW

**RENEWAL DATE:** November 2024

---

## 1. BACKGROUND

- 1.1. Confederation College is committed to providing high-quality education and services to our students, staff, community and preserving our reputational and financial integrity in order to continue our mission.
- 1.2. Enterprise Risk Management (ERM) is an ongoing, proactive and dynamic process involving the College's Board of Governors, management and other personnel. It is a systematic approach to setting the best course of action to manage uncertainty by identifying, analyzing, assessing, responding to, monitoring and communicating risk issues and events that may have an impact on the organization's ability to successfully achieve its strategic objectives.
- 1.3. The College has developed an ERM framework based on the internationally recognized principles from ISO 31000 to manage change and uncertainty. The framework applies to employees at every level and will assist the college in achieving its strategic objectives through structured and effective risk management processes.

## 2. DEFINITIONS

### 2.1 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 College from achieving its strategic priorities and supporting objectives, as well as positive risks that are in alignment with the College's strategic priorities and operational responsibilities.

2.2 **Risk**

Effect of uncertainty on objectives, deviation from the expected (positive and/or negative).

2.3 **Risk Appetite**

The amount of risk, on a broad level, an entity is willing to accept in pursuit of value.

2.4 **Steering Committee**

The Senior Team of Confederation College.

**3. PURPOSE AND OBJECTIVES**

- 3.1 The primary purpose of this policy is to articulate the College's approach to enterprise risk management (ERM) and provide an overview of the related roles, responsibilities, and accountabilities.

ERM is a common practice utilized by organizations across a variety of sectors, which aims to manage the risk necessary in the pursuit of strategic objectives. ERM forms part of the overall management system, helping to improve decision-making capabilities, prevent and mitigate risk throughout the College.

**4. POLICY STATEMENTS**

- 4.1. The College will establish and maintain an Enterprise Risk Management ("ERM") Program. In order to support the execution of the ERM Program, the College will maintain a Framework/Procedure and set of tools based on leading practice.
- 4.2 ERM will be executed through a systemic, ongoing process, with a view to supporting and facilitating the achievement of the College's objectives through the regular identification, analysis, treatment and monitoring of key risks.
- 4.3 The College will align its ERM Program on the most up-to-date ISO 31000 standard.
- 4.4 The College will promote a culture of risk management, which seeks to be proactive regarding risk. As appropriate, the College will seek to prevent or mitigate the impact of losses occasioned by negative risks, while supporting the informed and controlled undertaking of positive risks, in alignment with the College's strategic priorities and operational responsibilities. To this end, ERM will form a part of the overall management processes and risk information will be leveraged as much as possible to help inform decisions.

- 4.5 Within the ERM Program, risk information will be consolidated and reported on a regular basis to the Steering Committee, the Audit Committee and the Board with an aim to providing timely and appropriate information to enable effective and informed decisions.
- 4.6 The College will work to define the acceptable level of risk it is willing to assume in the pursuit of value through the documentation of Risk Appetite. The College's Risk Appetite will be reviewed regularly, updated as required and communicated to promote an appropriate culture of risk management.
- 4.7 The work performed within the ERM Program by any of the named groups will not replace any of the operational and tactical risk management happening in faculties and departments throughout the College.

## **5. ROLES AND RESPONSIBILITIES**

The following groups will have responsibilities within the ERM Program:

- 5.1 **The Board of Governors** have ultimate accountability for risk and risk management.
- 5.2 **The Audit Committee of the Board of Governors** will provide oversight of ERM Program and monitor 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 College's risks.
- 5.3 **The President** will appoint an ERM Steering Committee, who will oversee the implementation and ongoing execution of the ERM Program. The ERM Steering Committee will provide regular reports to the Audit Committee of the Board of Governors.
- 5.4 **The President** will appoint an ERM Workgroup, who will lead the completion of institution-wide risk assessments, mitigation and monitoring of enterprise risks. The ERM Workgroup will provide regular reports to the ERM Steering Committee.

## **6. REPORTING**

- 6.1 The Audit Committee of the Board of Governors receives and approves, an annual update of the enterprise risk management process and risk registry. This update includes details of high and extreme risks and provides the committee with additional reports to enhance their understanding of the process and the results of the process.

## **7. MONITORING**

- 7.1. The Board will receive an annual report from the Audit Committee identifying the high and extreme risks and confirming that satisfactory mitigation strategies are in place. The Board and Audit Committee will also receive a heat map identifying the number and category of all risks without the specific detail of each risk.

**8. RELATED DOCUMENTS**

- 8.1 Ministry's Binding Policy Directive – Governance and Accountability
- 8.2 College's Enterprise Risk Management Framework (**Attached**)

## ENTERPRISE RISK MANAGEMENT FRAMEWORK

### 1 Introduction

#### 1.1 Background

Confederation College has in place an Enterprise Risk Management (ERM) Program, with the aim of helping to effectively assess, communicate and manage risks across the Institution. Utilizing an institution-wide approach to risk management is a key part of the management system and a focus for the Board of Governors, the President and senior leadership, in line with our vision and strategic goals.

ERM is a common practice utilized by organizations across a variety of sectors; it forms part of the overall management system, helping to improve decision-making capabilities at all levels of the College. This document forms part of the College's overall ERM Program, which is established by the Enterprise Risk Management Policy.

#### Objectives

The overarching objectives of ERM at the College are to:

- Provide information to help inform risk-based decisions;
- Promote strategic effectiveness;
- Sustain the value the organization provides its stakeholders;
- Provide a methodology for evaluating new initiatives;
- Enable the avoidance of big mistakes or missed opportunities; and
- Promote proactive risk mitigation and action.

#### Alignment to ISO 31000 Risk Management – Principles and Guidelines

The College aligns its ERM Program to the ISO 31000 standard. The ISO standard is considered to be a leading practice for risk management and allows for effective integration and alignment of other standards adhered to at the organization. It ensures that the College is aligned with industry best practices and it provides opportunities to enhance the ERM on an ongoing basis.

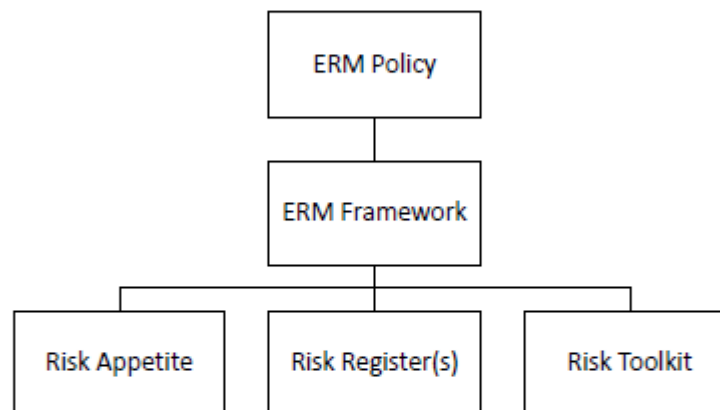
## 2 ERM Program Infrastructure

### 2.1 Overview

The ERM Program Infrastructure establishes the structures for the formal management of enterprise risks at the College. The Infrastructure specifically outlines the flow of documentation and participants' roles and responsibilities. This ensures the correct tools are in place to enable effective assessment, treatment and monitoring of institution-level risk. It has been designed to manage both positive and negative risk (also known as opportunities and threats).

### 2.2 Documentation Structure

ERM documentation is structured and designed to guide the process and ensure the College can identify and prioritize its areas of highest risk in order to drive the appropriate action required. The ERM Program follows the structure as outlined below.



A description of each of these elements can be found below and in the [glossary](#) of terms:

**ERM Policy** – a policy which outlines the College’s approach to Enterprise Risk Management.

**ERM Framework** – a document which outlines how the College applies and utilizes Enterprise Risk Management; this document represents the ERM Framework.

**Risk Appetite** – a summary of the amount of risk that the organization is willing to take in the pursuit of value; see [section 2.4](#) of this document for more information.

**Risk Register(s)** – is a record of information about identified risks; a register forms one of the key tools in risk management acting as a repository for all risks identified and includes additional information about each risk (e.g. nature of the risk, reference and owner, mitigation measures).

**Risk Toolkit** – a set of tools which are used in the execution of the ERM Program and processes; see [Appendix B](#) for more information.

### 2.3 Basis for Viewing & Managing Enterprise Risk

Strategic planning at the College is based on the achievement of its mission and strategic goals. While the specifics of the strategic goals may evolve over time to respond to the environment, the day-to-day utilization of the program remains objectives-based.

The basis upon which enterprise risks and opportunities for innovation will be viewed and managed will be dependent on how they integrate with the identified strategic goals. Assessing how individual risks, or a group of risks, may positively or negatively impact strategic direction will be the basis for risk evaluation and prioritization.

#### 2.4 Risk Appetite

Risk appetite refers to the amount and type of risk that an organization is willing to pursue or retain. It provides an important, forward-looking perspective and is a guide to risk management activities at the College when determining how much risk is acceptable. Risk appetite reflects the Institution's mission, vision and values, considers stakeholder expectations, the current state of the economy and higher education, and in turn, has an influence on both the culture and operations of the College.

Risk appetite will be established and reviewed on an annual basis to ensure that it continues to be aligned with the strategic direction.

#### 2.5 Program Governance

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

The Audit Committee of the Board of Governors provides oversight of the ERM Program and monitors the management of key/top risks. The Audit Committee will keep the broader Board of Governors abreast of key developments in the College's risks at a frequency identified in the ERM Policy and Terms of Reference.

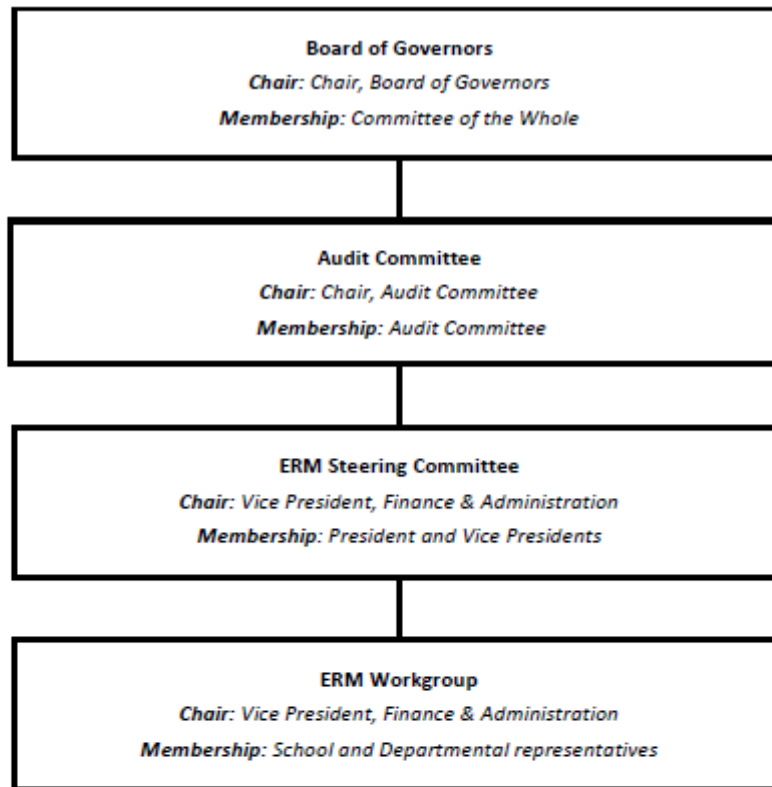
The ERM Steering Committee provides leadership, commitment and assumes overall responsibility and accountability for ERM, and the integration of associated processes into strategy. The Vice President, Finance & Administration will act as the Chair of the ERM Steering Committee and will present risk information on a regular basis to the Audit Committee as outlined in the ERM Policy and Terms of Reference.

The ERM Workgroup 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 College schools and departments. The Workgroup will be tasked with the formulation of College-wide risks based on both 1) information from departments and 2) their own assessment. The Vice-President, Finance & Administration (or a designate) will act as the Chair of the ERM Workgroup and will present risk information on a regular basis to the ERM Steering Committee.

Risk Champions will be identified, assigned risks and tasked with the monitoring and management of their risks. Risk Champions will assess, mitigate and monitor their respective risks and provide information on their risks to the Workgroup with regular frequency, as outlined in the reporting requirements.

#### 2.6 Governance Structure

The image below depicts the governance structure of the ERM Program at the College.



## 2.7 Roles & Responsibilities

The section below summarizes the roles and responsibilities related to the ERM Program.

### 2.7.1 Board of Governors

- Overall ownership and accountability for risk
- Monitor compliance with the risk management processes
- Review and utilize Risk Appetite statements
- Review status updates for key risks
- Integrate risk into Board decisions

### 2.7.2 Audit Committee of the Board of Governors

- Oversight of the ERM process
- Monitor the management of key/top risks
- Participate in the assessment of risks and development of mitigation strategies as required
- Review status updates for key risks
- Integrate risk into Board decisions
- Monitor emerging conditions or control weaknesses for key risks

### 2.7.3 ERM Steering Committee

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



- Establish and monitor risk appetite
  - Review risks assessed by the ERM Workgroup
  - Identify, analyze and action risks and opportunities in addition to those provided by the ERM Workgroup, including ad hoc, confidential and time-sensitive items
  - Oversee the development and execution of risk treatment strategies and mitigation projects
  - Act as Risk Owners of risks and controls within their areas of responsibility and validate/oversee treatment measures
  - Provide direction to the ERM Workgroup
  - Appoint a Chair of the ERM Workgroup and select members
  - Ensure ERM is linked to strategic goals
  - Ensure appropriate resources and level of effort required to implement and operate ERM
  - Report regularly to the Audit Committee
- 2.7.4 Chair of the ERM Steering Committee
- Lead the ERM Steering Committee
  - Ensure the review of the key/top risks as provided by the ERM Workgroup
  - Triage items to determine the need for action on the part of the Committee (including emergency meetings) ad hoc, confidential and time-sensitive risks and opportunities
  - Lead the assessment of ad hoc, confidential and time-sensitive risks and opportunities with the Committee
  - Facilitate reporting to the Audit Committee and Board of Governors, including cyclical and as needed reports
- 2.7.5 ERM Workgroup
- Identify, assess and monitor risks
  - Act at the direction of the ERM Steering Committee on risk management initiatives (e.g. ad hoc assessments of risks and/or opportunities)
  - Complete and maintain the College-wide Risk Register
  - Execute risk mitigation strategies and projects as applicable
  - Provide guidance and training related to risk management activities as required
  - Facilitate action in those areas where improvements are required to the ERM process
  - Report regularly to the ERM Steering Committee
- 2.7.6 Chair of the ERM Workgroup
- Lead the ERM Workgroup
  - Ensure the College-wide Risk Register is complete and maintained
  - Sit as a member of the ERM Steering Committee
  - Facilitate reporting to the ERM Steering Committee
  - Liaise with the ERM Steering Committee on a regular basis to ensure ERM Framework and process is functioning as intended
- 2.7.7 Risk Owners
- Assume accountability ('ownership') for risks and controls within their areas of responsibility
  - Identify new opportunities related to the risks within their areas of responsibility as applicable
  - Liaise with the Risk Champion regarding 'owned' risks

- Execute risk mitigation strategies and projects as applicable
- Account for resources (if applicable)

**2.7.8 Risk Champions**

- Liaise with the Risk Owner of risks within the areas they represent
- Provide updates to the Workgroup on ‘championed’ risks
- Facilitate reporting of risk information to the Workgroup
- Consult on risk for new projects and initiatives, ensuring risk is considered and evaluated

**2.7.9 Staff**

- Participate in risk assessment and treatments as requested
- Raise potential risks or opportunities to the ERM Workgroup

**2.8 Application of ERM & Reporting**

An effective ERM Program utilizes both regular cyclical assessment/management and an ability to execute analyses on key areas in an as needed manner for situations that are ad hoc, confidential and time sensitive. The College will utilize both approaches in its ERM Program. The same core process – outlined in [Section 3](#) of this document – will be utilized for both regular cyclical assessment/management and as needed/ad hoc requests.

**2.8.1 Regular ERM Cycle**

The College’s regular ERM cycle will run quarterly and will be centred on the work completed by the ERM Workgroup. The cycle will be aligned – as best as possible – to regular College operations (e.g. Board reporting, budgets, strategic planning, etc.).

Regular reporting is required to effectively monitor risks. The College will report the risk information gathered during its regular ERM Cycle as detailed in the table below. Guidance on the escalation of items can be found in [Appendix C](#). It is important to note that additional reporting will be provided upon request of ERM Steering Committee, the Audit Committee and/or the Board of Governors.

Report Recipient	Type of Risk Management Information	Reporting Responsibility	Timing
Board of Governors	ERM Program Status Update	Chair of Audit Committee	Semi-annually
Audit Committee	ERM Program Status Update	Chair of ERM Steering Committee	Quarterly <sup>1</sup>
	College-wide Risk Register	Chair of ERM Steering Committee	Semi-annually
ERM Steering Committee	College-wide Risk Register	Chair of ERM Workgroup	Annually
	Status Update for Key Risks	Chair of ERM Workgroup	Quarterly
ERM Workgroup	Departmental Risk Information	Risk Champions	Quarterly

<sup>1</sup> To be completed in line with the review of the Executive Limitations reporting

#### 2.8.2 Ad hoc, Confidential and/or Time Sensitive Situations

The need will arise – whether due to new initiatives, potential opportunities, or unforeseen issues – for review, assessment and/or action to be taken on key risk assessment to be completed outside of the Regular ERM Cycle as described above. It is the intention of the College to ensure that the ERM Steering Committee be aware of and provide guidance related to all significant or potentially significant risk items. Therefore, if any member of the staff become aware of situations which might be a significant risk to the College, they should notify members of the ERM Workgroup or leadership, who will in turn notify members of the ERM Steering Committee. The ERM Steering Committee will triage situations and determine the path forward, whether that be no action, specific action by a group/department (such as ERM Workgroup or the ERM Steering Committee itself) or action by the College as a whole.

#### 2.9 Awareness & Communication

Awareness and communication are critical to the successful implementation and on-going operation of ERM at the College.

To ensure all those with stated roles and responsibilities acquire and maintain the skills and knowledge needed for them to employ risk and innovation management activities, training will take place on ERM policy, 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 in the Workgroup to receive supplemental training and guidance on risk assessment, while those on the ERM Steering Committee receiving additional focus on risk governance and oversight.

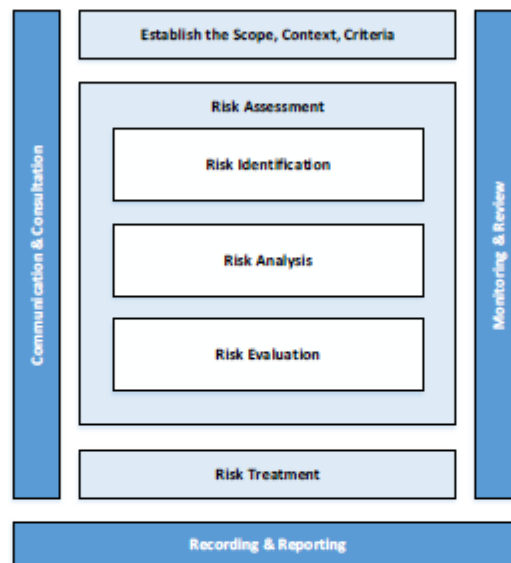
### 3 The Risk Management Process

#### 3.1 Overview

Key to successful risk management is a structured process and approach. The process used at the College aligns to ISO 31000. 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. Supporting information and guidance on the process is found in the Risk Toolkit.

#### 3.2 The Process

The information below outlines the risk management steps.



Specific steps within the process are outlined below.

##### 3.2.1 Communication & Consultation

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

##### 3.2.2 Establish the Scope, Context, Criteria

When establishing the context within its risk management process, the College will take into consideration the specifics of the current situation, 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.

### 3.2.3 Risk Assessment

Risk assessment consists of three (3) main steps and will result in the understanding of the risk exposure present. The steps of a risk assessment are outlined below:

- **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.
- **Risk Analysis:** Risk analysis allows the College to consider the extent to which potential risks might have an impact on the achievement of strategic goals. 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 Risk Register. This is known as the Probability-Consequence model of risk management.
- **Risk Evaluation:** Once risks are identified and analyzed in accordance with the previous steps, a Risk Register is further developed. The College will use a Risk Register as the primary tool for articulating its risk profile.

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

- Probability and/or consequence of risk being so low that specific mitigation plans are not required
- The risk being such that there are no mitigation actions available
- Cost of mitigation plan is excessive as compared to the benefit such that acceptance of the risk is the only option
- The risk is being driven by an external event/organization and therefore outside of the control of the College

### 3.2.4 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 ERM Steering Committee will oversee the development and execution of risk treatments. Once the optimal risk treatment is determined in the circumstance, the College 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 the College understand the significant risks that may negatively impact it and the stated strategic goals. 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:

- *Avoidance* – taking action to exit the activities that give rise to the risks
- *Control* – reducing the risk probability, consequence, or both
- *Transfer* – transferring or sharing a portion of the risk
- *Acceptance* – taking no action to affect probability or consequence

#### 3.2.5 Monitoring & Review

Regular monitoring and review of risks are essential to understanding the changing dynamic of risk. The ERM Steering Committee will monitor risks, provide updates to the Board of Governors and update the risk information as applicable with input from Risk Champions.

#### 3.2.6 Recording & Reporting

Throughout the risk management process, the ERM Workgroup and the ERM Steering 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.

## 4 Appendix A – 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 of the 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 (also referred to as ‘assessment criteria’)

**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 – positively or negatively – by a decision or activity



## 5 Appendix B – Toolkit

The ERM Toolkit will be maintained by the ERM Workgroup. It is comprised of the main tools that are utilized in the facilitation of the ERM Program. These tools will be managed through a site and be comprised of MS Office based templates.

Key components of the ERM Toolkit include:

- ERM Assessment Criteria
- ERM Steering Committee Terms of Reference
- ERM Workgroup Terms of Reference
- Risk Assessment Aide Memoire
- Risk Register Template
- Risk Worksheet

## 6 Appendix C – Risk Escalation

The table below provides an outline of the interpretation of the risk scores which are determined using the Probability-Consequence model (including actions for different scores).

Assessment	Score	Escalation	Management	Frequency of Review	Reporting
Low Risk	(1- 4)	No escalation required	No action required	Subject to annual review	As required updates to applicable parties
Moderate Risk	(5-11)	No escalation required	If risk level is deemed unacceptable, the enterprise risk is to be managed by the applicable subject area	Subject to annual review	Quarterly updates to the ERM Workgroup
High Risk	(12-18)	Requires timely escalation to the ERM Steering Committee	If risk level is deemed unacceptable, the risk is to be managed by the applicable ERM Steering Committee member	Subject to quarterly review	Quarterly updates to the ERM Steering Committee; may be included as part of the quarterly report to the Audit Committee at the discretion of the ERM Steering Committee
Critical Risk	(19-25)	Requires immediate escalation to the Audit Committee	If risk level is deemed unacceptable, the risk is to be managed by the applicable ERM Steering Committee member	Subject to monthly review	Monthly updates to the ERM Steering Committee; will be included as part of the quarterly report to the Audit Committee