Policy Title:	Enterprise Risk Management		
Category:	☒ Institutional - Board ☐ Institutional - Administrative	☐ Academic - Administrative ☐ Employment - Administrative	
Approved by:	☒ Board	☐ President	
Date approved:	October 19, 2018	**Effective date:**	October 19, 2018
Policy Sponsor:	Board Governance Committee Chair and President (co-sponsors)	**Date last reviewed:**	January 2019
Date of Mandatory Review (expiry date)	October 2021	**Date of last revision of Procedures**	August 31, 2017

1 POLICY

CMCC considers enterprise risk management (ERM) to be fundamental to good management practice and a significant aspect of corporate governance. Effective management of risk will support and contribute to the achievement of CMCC's strategic and operational goals and objectives.

1. CMCC will create an environment that proactively identifies opportunities and threats, and supports and encourages their assessment, mitigation and monitoring on an ongoing basis.

2. Enterprise risk management will form an integral part of CMCC's decision making processes and routine management and will be incorporated within the strategic and operational planning processes at all levels.

3. A CMCC Risk Register will be used to document and assess risks across the institution and will be reviewed semi-annually by the Executive Leadership Team.

4. A Strategic Risk Register will be updated annually and reported on formally to the Board of Governors.

2 PURPOSE

To develop an organizational culture of risk awareness, continuous quality improvement and safety for all through a framework for integrating ERM within operations to empower and encourage the use of the ERM process to proactively identify and manage institutional risks.

3 SCOPE

Employees and students.

4 INFORMATION AND COMPLIANCE PLANS (not a comprehensive list)

CMCC's strategic goals and outcomes will be achieved through deployment of an ERM program based on the following ERM framework:

The ERM framework outlines the processes by which CMCC will assure that its ERM policy and procedures are fully integrated within operations and that all business activities and decision making is aligned with the ERM process. This framework includes:

1. education and training on ERM for all
2. approval and periodic review of the ERM policy
3. adoption of the ERM process to monitor overall results and outcomes
4. specification of the role and responsibilities for CMCC's Chief Risk Officer
5. review of risk criteria proposed by management
6. review and approval of the risk profile
7. review of key risk indicators
8. implementation of black swan reviews.

CMCC will build its ERM program based on best practices from leading authorities, including ISO 31000 and COSO (2016).

5 RELATED POLICIES (not a comprehensive list)

- CMCC Code of Conduct

6 DEFINITIONS

Black swans are rare, unexpected, high impact events that are highly unlikely but should they occur could have a disastrous impact on the institution.[i]

Enterprise risk management is the coordinated activities to direct and control an organization with respect to risk.[ii]

The ERM process is the steps involving scanning the environment for risks, risk assessment, risk treatment and the monitoring of the results from risk treatment.

Key risk indicators are the metrics used to project impending risk situations.[iii]

Risk is the effect of uncertainty on objectives.[iv] Risk can be positive or negative. Risk can either be transferred to third parties through risk sharing, insurance, contracts or waivers or mitigated by implementing internal risk management strategies, or it can be ignored.

Risk assessment includes the steps of risk identification followed by risk analysis and risk evaluation.[v]

Risk classifications are the four quadrants of risk, including: hazard, operational, financial and strategic risk.[vi]

Risk criteria are the terms of reference against which the significance of a risk is evaluated. Risk criteria are the internal procedural rules to determine and express the magnitude of a risk and to judge its significance against predetermined levels of concern.[vii] CMCC will utilize its Risk Grid to assign a risk score to identified risks (see Risk Register and Risk Grid template, attached).

The Risk Register is the official record which documents identified risks and the results of risk assessment, treatment, and monitoring produced at the management level and consolidated at the organizational level (see Risk Register and Risk Grid template, attached).

New Policy Approved (date):
August 31, 2017 by Administration
October 19, 2018 by Board (no revisions)

Policy Revision History (dates):

----------**END OF POLICY**----------

7 PROCEDURES

1. All employees, students and those governed by CMCC policies from time to time are encouraged to identify and raise questions or concerns about institutional risks and to bring these forward to an individual who is serving in a management capacity.

2. The ERM process is activated as needed and as scheduled throughout strategic and business planning processes, decision making activities, operational reviews including results of internal and performance audits, including accreditation, initiation of new projects and contract approvals, any business change initiative undertaken, etc.

   The following outlines the formalized five step ERM process for CMCC:

   Step 1 Scan the environment for risks
   Step 2 Identify risks
   Step 3 Analyze and evaluate risks
   Step 4 Treat risks
   Step 5 Monitor the results

   Step 1: Scan the environment for risks

   Division Directors are responsible for facilitating a review with their staff of both the internal and external environments for strategic, financial, operational and hazard risks which may impact the achievement of organizational objectives. By doing so, it will be possible to classify risk.

- Examples of external environment factors include: economic environment; political climate; legal and regulatory, including the Accessibility for Ontarians with Disabilities Act, 2005 (AODA), privacy, accreditation, etc.; technology; natural environment; competition; occupational health, wellness and safety protocols; emergency management, etc.

- The internal environment factors consist of: the organizational culture; vision, mission and values; risk appetite – willingness of the organization to accept risk; organizational structure; operations, including people, processes and systems; availability of resources; policies and procedures; communication and consultation; reporting channels, etc.

   Step 2: Identify risks

   Division Directors through and by consultation with staff and others, and Board Committee Chairs through and by consultation with their committees, are responsible for identifying existing and key emerging risks and recording them in CMCC's Risk Register.

Step 3: Analyze and evaluate risks

Division Directors and Board Committee Chairs are responsible for conducting a risk assessment on identified risks. Risk assessment is a two-part process which involves risk analysis and evaluation.

a. Risk analysis involves determining the potential sources and the causes of the risk and the likelihood and impact of the risks. Risk likelihood and impact are determined using the Risk Grid to assign a Risk Score to each risk item (see Risk Register and Risk Grid template, attached).

b. Risk evaluation involves determining whether the risk is tolerable/acceptable or not when that risk is measured against best practices. Risk evaluation involves measuring the variation/difference/gap between the existing level of risk (prior to risk treatment) against what would be the acceptable/tolerable level of risk.

Division Directors and Board Committee Chairs will document the results of the risk assessment, risk analysis and risk evaluation in their divisional or committee Risk Register.

Step 4: Treat risks

Division Directors and Board Committee Chairs are responsible for making a decision on how to treat the identified risks.

Risk treatment involves determining the most appropriate option for the risk, including whether or not to treat the risk. Typical risk treatment decisions include:

- Avoid the risk, by not initiating or continuing the activity giving rise to the risk
- Modify the risk, by changing the likelihood and/or the impact of the risk
- Retain the risk, which may involve altering the existing internal controls
- Transfer the risk, through insurance or sharing with another party or parties (such as using contracts)
- Exploit the risk, by taking it in order to pursue an opportunity.

Risk treatment involves developing an action and implementation plan to treat the risk and determining who is responsible for implementing the plan's recommendations. Risk treatment plans indicating who is responsible are to be documented in the CMCC Risk Register.

Step 5: Monitor the results

Division Directors and Board Committee Chairs are responsible for monitoring the results of risk treatment actions.

Risk monitoring involves reviewing risk treatment action and implementation plans and recommendations to alter the risk. The purpose of risk monitoring is to determine whether the action and implementation plan to treat the risk have been effective in altering the level of risk. Monitoring of results is to be documented in the CMCC Risk Register.

[i] The Handbook of Board Governance
[ii] ISO 31000:2009 International Organization for Standardization
[iii] The Handbook of Board Governance
[iv] ISO 31000:2009 International Organization for Standardization
[v] Risk Management Principles and Practices – The Association of Risk Managers
[vi] Risk Management Principles and Practices – The Association of Risk Managers
[vii] ISO 31000:2009 International Organization for Standardization

New Procedure Approved (date):
August 31, 2017 by Administration
October 19, 2018 by Board (no revisions)

Policy Revision History (dates):

8 ATTACHMENTS

1. Risk Register
2. Risk Grid

RISK REGISTER

NAME OF DEPARTMENT
NAME OF DIRECTOR/DEAN
Prepared by
Date - last updated

	Short Description of Risk	A. Risk Classification	B. Impact Score	C. Likelihood Score	Risk Score	Existing Controls	Risk Tolerance	Treatment Action	Person Responsible	Risk Monitoring Results
1										
2										
3										
4										
5										

please add more rows if there are more risks identified

A. Risk Classification

HAZARD RISK	OPERATIONAL RISK	FINANCIAL RISK	STRATEGIC RISK
Insurance deals primarily with hazard risk			
Property Risk - Uncertainty related to loss of wealth due to damage or destruction of property	**People Risk** - All the employees of an organization including contractors, vendors, clients involved in selecting the right people	**Market Risk** - Arises from change in the value of financial instruments	**Economic Environment** - The macroeconomic environment in which the organization operates produces many effects on the organization such as inflation, financial costs
Examples - theft, damage/destruction from accidents and weather to real and personal property as well as intangible property	*Examples - All the procedures and practices organizations use to conduct their business activities and the deviations from these processes*	*Examples - Currency price risk for organizations operating in more than one country, interest rate risk owing to the change in interest rates, commodity price risk, equity price risks related to the organizations investments in external stock and other securities and liquidity price risk related to its ability to raise cash*	*Examples - Inflationary cost escalation, environment, critical incidents, economic/social changes, advances in technology*
Liability Risk - Uncertainty related to financial responsibility arising from bodily injury including death or loss of wealth that a person or organization causes to others	**Process Risk** - All the procedures and practices organizations use to conduct their business activities and the deviations from these processes	**Price Risk** - The potential for a change in revenue or cost because of an increase or decrease in the price of a product or input	**Political Environment** - Any action by government
Examples - damages related to successful claims, settlement costs, legal fees and court costs	*Examples - Policies and procedures, internal controls, internal and external review, analysis of errors, management processes*	*Examples - Price charged for the organizations services (tuition fees) and products (purchases) and the price of assets purchased and sold*	*Examples - Lack of political support, legislative changes, regulatory developments*
Personnel Risk - Uncertainty related to the loss due to death, incapacity or prospect of harm to or unexpected departure of key employees that deprives the organization of the person's special skill or knowledge that organization cannot readily replace	**Systems Risk** - Risks associated with technology and equipment	**Credit Risk** - Borrower defaults, student default on tuition	**Demographics** - The statistical characteristics of nations such as increasing life expectancy, aging of population
Examples - key person's death, disability, retirement or resignation	*Examples - Testing and monitoring, information/data security, availability/access to information, IT systems*		*Examples - Demographic changes*
	External Events - Such as business disruptions, loss of key supplier, utility failure		**Competition** - Between organizations and nations
			Examples - Increased competition and squeezed margins, reputation, student outcomes

B. Impact

Score	Impact	Description
1	Insignicant	Very limited number of events, limited loss, limited damage, negligible, minor disruption
2	Minor	Limited number of events, minor injuries or damage, normal difficulty, minor setback, some unfavorable attention, minor cost overruns
3	Moderate	Moderate number of events, serious injuries or moderate damage, delays, moderate disruption, some loss of service, moderate cost overruns, some loss of trust, negative attention, negative audit or outcome rating
4	Major	Major number of events, loss of major asset, serious injuries or major damage, program/project redesign required, major disruption of essential services, major cost overruns, major loss of trust, public outcry for change, strong criticism in audit
5	Catastrophic (Significant or Extreme)	Significant number of events, public affected, significant or extreme funding decrease, significant damage, death or significant disability, program/project irrevocably finished (objectives not met), essential services disruption for extended periods, total loss of service or data, extreme cost overruns, public call for change, internal vote of non-confidence, very negative public ratings

C. Likelihood

Sc.	Likelihood	Description
1	Rare, Improbable	May occur in exceptional circumstances
2	Unlikely	Could occur if circumstances change
3	Possible	Might occur under current circumstances
4	Likely	Will probably occur in most circumstances
5	Almost Certain	Is expected to occur unless circumstances change

RISK GRID

		Risk Grid				
I						
M	Catastrophic	5	10	15	20	25
P	Major	4	8	12	16	20
A	Moderate	3	6	9	12	15
C	Minor	2	4	6	8	10
T	Insignificant	1	2	3	4	5
		Rare	Unlikely	Possible	Likely	Almost Certain
		Likelihood				