| | | | |
|---|---|---|---|
| **Policy Title:** | Enterprise Risk Management | | |
| **Category:** | ☒ Institutional - Board<br>☐ Institutional - Administrative | ☐ Academic - Administrative<br>☐ Employment - Administrative | |
| **Approved by:** | ☒ Board | ☐ President | |
| **Date approved:** | April 22, 2022 | **Effective date:** | April 22, 2022 |
| **Policy Sponsor:** | Board Governance Committee Chair and President (co-sponsors) | **Date last reviewed:** | April 22, 2022 |
| **Date of Mandatory Review (expiry date)** | April 2027 | **Date of last revision of Procedures** | April 22, 2022 |

## 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 a continuous and 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. An annual update of the Risk Register will be reported 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, students and those governed by CMCC policies from time to time.

## 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)

- Code of Conduct - Employees

## 6 DEFINITIONS

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

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.[ii]

Risk is the effect of uncertainty on objectives.[iii] 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.[iv]

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

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.[vi] 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).

Unprecedented and unexpected events are rare and high impact events that are highly unlikely but should they occur could have a disastrous impact on the institution.

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

**Policy Revision History (dates):**
February 24, 2022 by Administration
April 22, 2022 by Board (no revisions)

----------**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 framework is continuously in an active state throughout strategic and business planning processes, decision making activities and operational reviews including and not limited to results of internal and performance audits, institutional accreditation reviews, initiation of new projects and contract approvals, and considered as part of any operating unit change initiative.

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

   Step 1 Environmental scan of suspected and/or potential risks
   Step 2 Identify risks for purposes of conducting a comprehensive risk assessment
   Step 3 Analyze and evaluate risks
   Step 4 Identify, develop and implement risk mitigation measures
   Step 5 Monitor impacts and reassess risk levels

   To ensure clarity, each step in the ERM process is outlined below:

   **Step 1: Environmental scan of suspected and/or potential risks**

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

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

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

**Step 2: Identify risks for purposes of conducting a comprehensive risk assessment**

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: Identify, develop and implement risk mitigation measures**

Persons in a leadership role (e.g. Executive Leadership Team and Division Directors) are responsible for making decisions relating to identification, development and implementation of risk mitigation measures.

Risk mitigation measures involve determining the most appropriate institutional approach to managing the risk(s), including whether or not to develop and implement risk mitigation measures. Some risk mitigation strategies include:

- Avoid element(s) identified as potential risks, by not initiating or continuing the activity giving rise to the risk
- Modify the risk, by assessing 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 contractors/contract personnel)
- Exploit the risk, acknowledging potential impacts and assessing this against benefits of pursuing an opportunity.

Developing risk mitigation measures also involves creating the necessary action and/or implementation plan to reduce the level of risk below an identifiable risk tolerance threshold. Risk mitigation plans must document the person(s) responsible within the CMCC Risk Register.

**Step 5: Monitor impacts and reassess risk levels**

Persons in a leadership role (e.g. Executive Leadership Team and Division Directors) are responsible for monitoring the impacts of risk mitigation measures that were implemented, while also reassessing levels of risk for purposes of determining any need for post-implementation or ongoing risk mitigation measures.

Risk monitoring involves reviewing risk mitigation measures and associated implementation plans that may have been intended to reduce the level of overall risk. The purpose of monitoring impacts and reassessing risk levels is to determine whether the risk mitigation measures were effective in altering the level of risk. Monitoring of impacts on risk is to be documented in the CMCC Risk Register.

---

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

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

**Procedure Revision History (dates):**
February 24, 2022 by Administration
April 22, 2022 by Board (no revisions)

## 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 | | | | |