OMA Ontario Medical Association

Enterprise Risk Management (ERM) Framework

Last Update: May 8th, 2023

OMA Ontario Medical Association

Table of Contents

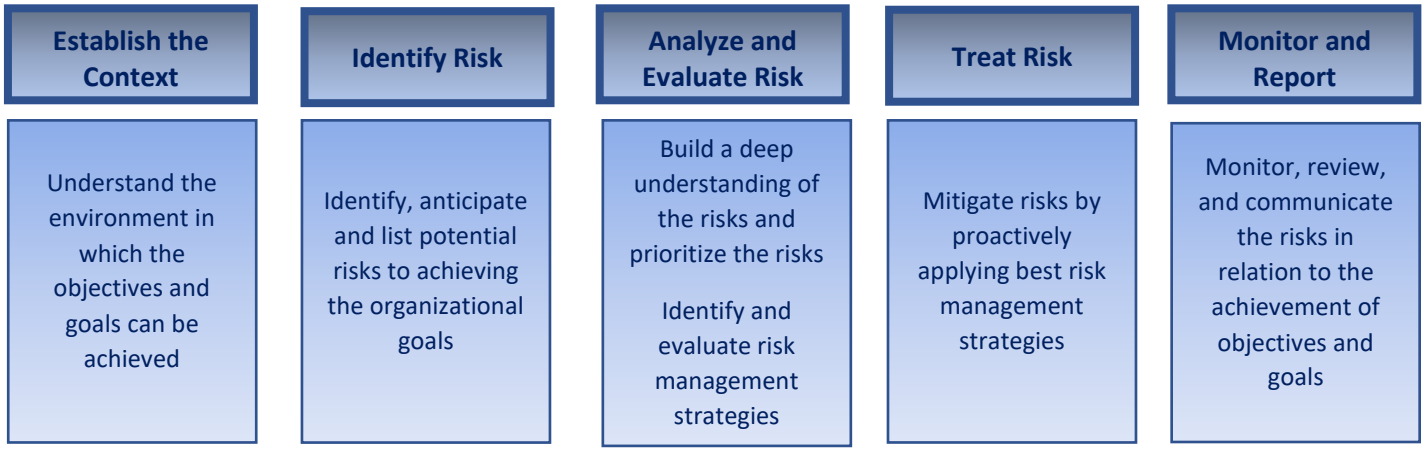
At a Glance: OMA ERM Framework

The Enterprise Risk Management (ERM) Framework, as set out in the OMA ERM Policy, describes risk governance and risk management processes that OMA can use to manage risks. The Framework can be scaled to fit each individual department and subsidiary, program area and initiative. By using the concepts and methodologies in the Framework, this will enable OMA to proactively anticipate and identify risks sooner and mange them effectively whenever possible before the risk event occurs and to respond to the event sooner when it occurs.

The Framework contains a total of nine Sections, and each Section is outlined in the table below. Further, Section 9 Risk Management Process is illustrated below.

Sections	Descriptions
1. Purpose	The purpose of the document, established by the ERM Policy, is summarized.
2. Principles	The OMA ERM principles, aligned with the international standards, are outlined.
3. Objectives	The ERM objectives are established to help manage risks that may threaten or enhance the achievement of OMA strategic objectives.
4. Program Infrastructure	The ERM documentation structures in place for enterprise risk management at OMA are described.
5. Risk Taxonomy	The organization / hierarchy of risk events by risk categories are defined for OMA.
6. Governance	The three lines of defense risk governance structure is illustrated.
7. Roles & Responsibilities	The ERM roles and responsibilities are described.
8. Reporting	The regular cyclical and ad-hoc, confidential and/or time sensitive ERM reporting requirements and escalation protocol are outlined.
9. Process	The structured risk management processes and approaches, aligned with ISO 31000, are described and outlined.
Appendix A: Glossary	Risk related terminologies pertaining to the OMA ERM Framework are defined.

Risk Management Process



1. PURPOSE

The Ontario Medical Association (OMA) has in place an Enterprise Risk Management (ERM) function, with the aim of helping to effectively assess, communicate and manage risks across the organization. Utilizing an enterprise-wide approach to risk management is a key part of the management system and a focus for the OMA Board, the Chief Executive Officer (CEO) and the Chief Financial and Operational Officer (CFOO), in line with our strategic goals and objectives.

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 within the executive and director levels, and in other layers of management. This document forms part of OMA's overall ERM Program, which is established by the ERM Policy, and is applied by OMA to:

- establish principles, objectives, processes, and governance structures that will enable OMA an overall oversight of ERM across the organization,
- provide foundations for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization, and
- take an integrated, holistic approach to enable OMA to manage risks across all levels and functions by proactively identifying and mitigating risks while becoming prepared to take planned actions for adverse situations as they arise to decrease negative consequences and to recover sooner.

2. ERM PRINCIPLES

Enterprise risk management is a continuous and active process at OMA that aids the identification, understanding and management of the key risks that can have the greatest impact, either positively or negatively, on the achievement of our strategic objectives. The ERM Policy is based upon the internationally recognized *International Organization for Standardization (ISO) 31000 Risk Management - Guidelines, Second Edition (2018)* and *Committee of Sponsoring Organizations (COSO) ERM – Integrating with Strategy & Performance (2017) Framework*.

The following are our ERM principles:

- We continuously pursue a holistic and integrated approach to managing risks across the organization;
- We actively pursue "risk as opportunity" in order to support our growth, improve overall membership service delivery, employee well-being, operational performance and resilience;
- We integrate ERM with our strategic planning and execution, operations, finance, people and culture, and legal / regulatory compliance processes;

- We continuously reinforce a culture that everyone, regardless of position and seniority, has a role to play in ERM and achieving our strategic objectives;
- We use risk management to help us develop innovative membership service delivery approaches to continuously improve our services and operations;
- We will put in place appropriate mitigation strategies which support our ability to achieve our goals and strategic objectives;
- We set clear risk accountabilities to manage risks across the 3 Lines of Defense (3LOD);
- We continually review our risk management activities and the effectiveness of our mitigation strategies to manage the key risks;
- We always seek shared perspectives and broader understanding of risks through active staff engagement, transparency, innovation and decision-making; and
- We continuously equip our people with the training, tools and capabilities to undertake their risk management roles and responsibilities.

3. ERM OBJECTIVES:

One of the primary purposes of ERM at OMA is to help us better manage the risks which may threaten or enhance the achievement of our strategic objectives. In order to ensure alignment of our risk management approach with our strategy, the following objectives have been established for ERM:

- Embed a structured and disciplined approach to identify and assess key risks and their potential impact on the achievement of OMA's strategic objectives;
- Establish risk management as part of OMA's existing governance, roles and responsibilities, and organizational structure;
- Enable risk-based consideration and evaluation of new strategic, service delivery and operational improvement opportunities;
- Implement a "multi-layered" risk management approach to manage, monitor, and report on the key risks that may have a significant impact on the achievement of OMA's strategic objectives. The process must support risk identification and mitigation at the strategic, service delivery, and operational and layers of OMA;
- Provide an overarching ERM framework that is linked to, and is integrated with other risk management related programs in-place within the organization;
- Promote collaboration between stakeholders to assess and manage risks that may impact our collective goals and shared responsibilities;
- Enable the Board of Directors and Executive Team to make risk-based decisions and allocate resources accordingly;
- Provide a constructive and forward-looking platform for the Board of Directors, the FAC, and Executive Team to identify and assess emerging risks as both "threats" and

"opportunities". Emerging risk assessments should fully inform multi-year strategic planning and yearly budgeting and operational planning; and

- Improve our risk management capabilities through continuous improvement, lessons learned, and adoption of industry leading practices.

Alignment to ISO 31000 Risk Management – Principles and Guidelines

OMA aligns it's ERM program to the ISO 31000 standard. The ISO 31000 standard is considered a leading practice for risk management and allows for effective integration and alignment of other standards adhered to at the organization.

4. ERM PROGRAM INFRASTRUCTURE

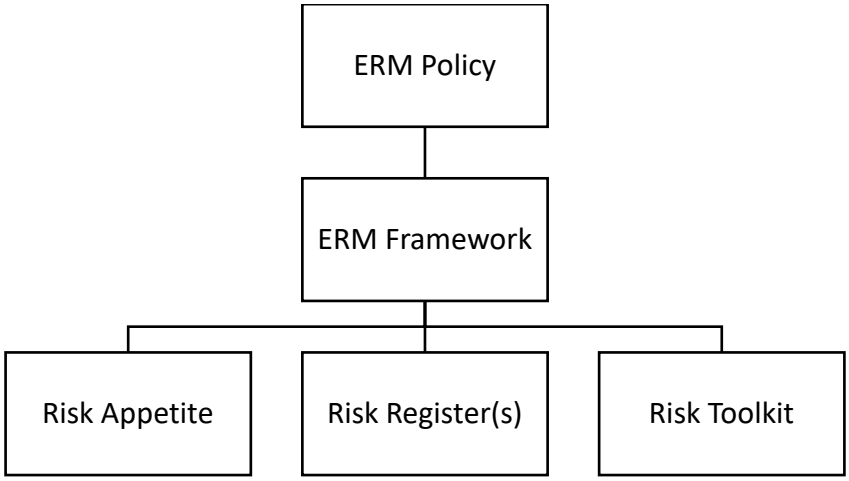
Overview

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

Documentation Structure

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

Figure 1: ERM Program Structure



A description of each of these elements can be found below:

ERM Policy – a corporate policy which outlines the OMA's approach to ERM.

ERM Framework – a document outlines how the OMA applies and utilizes ERM. This document represents the ERM Framework.

Risk Appetite – The amount of risk, on a broad level, an organization is willing to take in pursuit of value.

Risk Register(s) – is a formal 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. Some of the tools include, but not limited to, a risk register template, risk assessment criteria, risk assessment aide memoire, and other risk tools developed by Operational Excellence, ERM as the ERM Program matures.

Basis for Viewing & Managing Enterprise Risk

Strategic planning at OMA is an ongoing core activity that engages the organization and members in identifying goals, objectives and initiatives that delivers value to the membership. While the specifics of the strategic goals, objectives and initiatives may evolve over time to respond to the environment, the day-to-day execution of the strategy remains outcomes focused.

The basis upon which enterprise risks and opportunities will be viewed and managed will be how they integrate with the identified strategic objectives. Assessing how individual risks, or "risk themes," may positively or negatively impact strategic direction will be the basis for risk evaluation and prioritization.

5. RISK TAXONOMY

A Risk Taxonomy organises hierarchically risk events by risk categories (Level 1) and sub-categories (Levels 2) and is a foundational element of the ERM Program and practices across OMA. A Risk Taxonomy ensures that:

1. A common risk language is understood and spoken across the organization,
2. A high degree of completeness in the coverage of risks,
3. Users are encouraged to consider risk events and sources of risks versus breakdown in control (e.g. lack of succession plan) or impact (e.g. financial loss, reputational impact) may affect the OMA's strategic objectives,

4. The risk process (including risk assessment, monitoring, aggregation and reporting to Management and the Board) is well structured,
5. A structured perspective of risks is provided to external stakeholders, and
6. Risk roles and responsibilities for the key risks are allocated across OMA.

OMA has identified and defined the below listed risks at level 1:

Risk Taxonomy (Level 1)	Definition	Risk Taxonomy (Level 2) - Examples
Strategic Risks	Risks that arise due to uncertainties from business decisions, implementation of business decisions or responsiveness to external changes.	• Key Strategic Partnerships • Membership Growth • Change in Government • PSA Negotiations • Political • Resource / Capital Allocation • Membership Relevance • Governance • Subsidiary / Group Risk • Reputation
Financial Risks	Risks that would arise due to uncertainty surrounding the future investments / funds to meet OMA's investment goals.	• Access to Capital • Funding • Membership Revenue / Fees • Liquidity • Insurance • Pension • Investment
Operational Risks	Risks that would typically arise from the day-to-day conduct of the business from inadequate or failed internal processes, people and systems or external events that impact OMA's operating environment	• People & Culture • Information Technology • Information / Cyber Security • Privacy • 3-Party Management • Project Management • BCP
Legal & Regulatory Risks	Risks related to organizational, operational, legal, regulatory and compliance risks including changes in applicable laws and regulations that can affect OMA's businesses.	• Compliance • Regulatory Changes • Litigation • Fraud • Anti-Money Laundering

6. ERM GOVERNANCE

OMA has developed a risk governance structure that follows the three Lines of Defense (LOD) model and that is embedded within our existing organizational structure (***Appendix B***). The model depicts an ERM governance framework that splits responsibility for risk management across the following three lines:

- **1st LOD:** Front-line and relevant executive responsible to identify, analyze, evaluate, mitigate, monitor and report on key risks. This includes owning and managing risks and implementing corrective actions to address process and control deficiencies.
- **2nd LOD:** Control and oversight functions (e.g. Operational Excellence, ERM, Privacy Officer, and Executive Team) responsible to oversee and facilitate the risk management framework, process, and reporting to the Executive Team and to the Board, and to provide effective challenge to the 1st LOD. ERM Workgroup / ISTRO is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.
- **3rd LOD:** Assurance functions (e.g. Internal Audit), responsible to provide the Board and Executive Team with independent assurance on the adequacy and effectiveness of governance, risk management, and internal controls, including the manner in which the 1st LOD and 2nd LOD achieve risk management and control objectives.

It assigns clear ERM roles and responsibilities with appropriate independence and segregation of duties as outlined in the section below.

7. ROLES AND RESPONSIBLITIES

Some of the key roles and responsibilities of the OMA stakeholders include the following:

Board of Directors (Board)

- Oversee risk management efforts and practices.
- Delegate ERM oversight responsibilities to the FAC.
- Provide final approval on any FAC recommendations to the ERM Framework, methodology, resources, and other matters raised by the FAC.
- Discuss any matters that have been escalated by the FAC (e.g. breaches in risk appetite, changes in risk profile, etc.).

Finance and Audit Committee (FAC)

- Review and recommend updates to the ERM Policy and ERM Framework and supporting policies, standards, guidelines to Board for approval.
- Monitor compliance with the risk management processes.
- Approve delegation of risk limits to management and approve any transactions exceeding those delegated authorities.

- Oversight of the assessment of risks and provide guidance on mitigation strategies as required.
- Oversight of the assessment of opportunities and new initiatives, and provide guidance as required.
- Monitor emerging conditions for key risks and treatment plans.
- Review Risk Appetite Statements and metrics periodically or when there is a material change to OMA's operating environment.
- Review key risk report and status updates (e.g. status of action plans and trends).
- Review and approve allocation of ERM resources.

Executive Team

- Ensure ERM principle and mandates are integrated with strategic objectives.
- Assess ad hoc, confidential, and time-sensitive risks and opportunities as they arise.
- Analyze, and take appropriate decisions on risks and opportunities, including emerging and fast changing situations and events.
- Determine and establish a most balanced approach that enables the organization to effectively mitigate risks while taking advantage of opportunities to achieve the organization's strategic objectives with optimal cost and resource utilization.
- Oversee the development and execution of risk treatment and mitigation strategies developed in partnership with Operational Excellence, ERM to ensure appropriate decisions and treatments are in place.
- Ensure appropriate resources and level of effort required for an effective ERM Program are maintained.
- Ensure the FAC and the Board of Directors are informed of key and emerging risks.
- Oversee the development and execution of risk treatment and mitigation strategies developed in partnership with Operational Excellence, ERM to ensure appropriate decisions and treatments are in place.
- Review and validate the information and regular reports to the FAC and Board of Directors.
- Review and validate material changes to the ERM Framework, and supporting policies, standards, and guidelines.
- Delegate authority, responsibility, and resources to individual departments to identify and assign Risk Owners.
- Establish risk appetite and tolerance levels.
- Work closely with and provide support to their department ERM Workgroup representative to ensure proper risk management process within the department.
- Have an agenda item in existing department's management meetings to visit pertinent risks at appropriate interval on regular basis (e.g. quarterly).

Legal

Legal plays a critical role in all areas of legal, regulatory, compliance, and operational risk management. While Legal typically becomes involved in the critical and high-risk situations where there may be significant legal exposure to the organization, Legal concurrently monitors, prioritizes, and supports the organization with other non-critical and emerging legal exposure situations. Some of the examples of Legal role include the following:

- Oversee risk mitigation related to organizational and operational legal risks stemming from changes in applicable laws and regulations that can affect OMA's businesses.
- Lead, guide and support the organization related to legal, regulatory and compliance risk mitigation across the OMA as they are identified / raised by the OMA stakeholders.
- Lead, guide and support OMA with the development of appropriate polices, procedures and guidelines as needs arise.

Operational Excellence, ERM

- Coordinate and facilitate the annual enterprise-wide risk identification, prioritization and assessment process.
- Develop, maintain, and report on enterprise key risk register/report.
- Advise on current mitigation strategies/plan and providing recommendations on incremental/ planned mitigation strategies/plan.
- Coordinate with the Risk Owners to ensure adequate monitoring of the implementation of the incremental/planned mitigation strategies.
- Lead the Workgroup.
- Coordinate with Risk Owners to report on key risks, including new/emerging risks.
- Facilitate the preparation of the risk reports to the Executive Team and FAC / Board.
- Report directly to the CFOO, ET and FAC / Board.
- Act as an ERM knowledge resource and change agent across the organization.
- Obtain required resources to ensure the ERM Program is effective.
- Promote risk awareness and providing continuous education and training on risk management.

Enterprise Risk Management Workgroup (ERMW):

- Monitor, review and oversee operational risk management activities (identification, assessment, evaluation, mitigation, monitor and report) and the effectiveness of mitigation strategies to support the OMA's strategic goals in accordance with the ERM Policy, Risk Appetite Statements (RAS), and ERM Framework and other organizational policies as appropriate.
- Ensure that the operational risk information compiled through the standardized organizational ERM Risk Register tool is relevant, practical, and useful in supporting the decision-making process for the CFOO and ET at the organizational level.
- Facilitate the advancement of consistent risk management programs and tools across the OMA in support of OMA's strategic objectives.

- Foster a collaborative partnership risk culture by promoting organizational ERM perspectives, principles, and practices throughout the OMA.
- Ensure regulatory risk and compliance management programs are consistent with the best industry ERM practices, where appropriate.

Information Security & Technology Risk Office (ISTRO)

- Work in conjunction with Operational Excellence, ERM and individuals responsible for risk management processes at the OMA, the ISTRO focuses on IT risks, Cybersecurity, Business Continuity Planning, and Third-Party risk to ensure appropriate risk management strategies are in place to protect the organization from being impacted in these areas.
- Support the ERM Workgroup by providing advise on various considerations when addressing IT risk, cybersecurity, business continuity plans and third-party risk assessments.
- Provide IT, cybersecurity, business continuity planning and Third-Party risk expertise, advice, support, monitoring, and challenge to employees and management as required.

Risk Owners and Staff

- Assume responsibility ('ownership') for risks and controls within their areas of responsibility.
- Identify new opportunities related to the risks within their areas of responsibility as applicable.
- Provide updates to the Workgroup on 'owned' risks.
- Execute risk mitigation strategies and projects as applicable.
- Facilitate reporting of risk information to the Workgroup.
- Account for resources (if applicable).
- Participate in risk assessments and treatments as requested.
- Raise potential risks or opportunities to the ERM Workgroup, Operational Excellence, ERM or their respective Executive Team member.

Internal Audit

Provide core assurance to management and the Board on the effectiveness of adequacy and effectiveness of risk management at the OMA.

To maintain its independence, Internal Audit reports directly to the Board (via the FAC), and should not undertake or make any management decision with respect to the following ERM activities:

- Set the risk appetite.
- Manage assurance on risks.
- Take decisions on incremental/planned mitigation strategies.
- Implement incremental/planned mitigation strategies on the Executive Team's behalf.
- Accountable for developing and/or implementing ERM.

8. ERM REPORTING

An effective ERM Program utilizes both a 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. OMA will utilize both approaches in its ERM Program. The same core process will be utilized for both regular cyclical assessment / management and as needed / ad hoc requests.

Regular ERM Cycle

OMA's regular ERM cycle will run quarterly and will be the consolidated review of department risk registry information and Executive Team review to ensure key and emerging risks and their respective action plans are brought forward to the FAC and Board.

Regular reporting is required to effectively monitor risks. OMA will report the risk information gathered during its regular ERM Cycle as detailed in the table below. It is important to note that additional reporting will be provided upon request of the Executive Team, FAC and / or Board.

Report Recipient	Type of Risk Management Information	Reporting Responsibility	Timing
Board of Directors	Key Risk Report	Chief Financial and Operating Officer & Operational Excellence, ERM	Twice per year
	Update on State of ERM Program	Chief Financial and Operating Officer & Operational Excellence, ERM	Twice per year
Finance and Audit Committee	Update on State of ERM Program	Chief Financial and Operating Officer & Operational Excellence, ERM	Twice per year
Executive Team	Summary of the Department Risk Registers	Chief Financial and Operating Officer & Operational Excellence, ERM	Once per quarter
	Key Risk Report	Chief Financial and Operating Officer & Operational Excellence, ERM	Once per quarter

Ad hoc, Confidential and/or Time Sensitive Assessments

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

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 policy, procedures, tools, roles, and responsibilities.

It is vital that individuals receive appropriate training on the ERM Program, commensurate with their roles and responsibilities. By way of example, it will be necessary for those on the Workgroup to receive supplemental training and guidance on risk assessment, while those on the Executive Team receiving additional focus on risk governance and oversight.

It is the intention of OMA to ensure that the Executive Team 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 OMA, they should notify members of the ERM Workgroup or Executive Team. The Executive team will triage situations and determine the path forward, whether that be no action, specific action by a group/department or action by the OMA as a whole.

Escalation Protocol

The Operational Excellence team will escalate any changes in the following:

- Material changes to the key risk profile
- Significant delays in proposed mitigation strategies

Depending on the severity or the materiality of the change, the relevant information (assessment, implication, mitigate (action plan) will be reported and escalated as follow:

Breach Type	Severity / Materiality	Accountable Stakeholder	Reporting Group	Next Steps / Actions
Material changes to the key risk profile	Additional Risks	Risk Owner	ET and FAC	Prompt escalation to the immediate next reporting level with rationale(s), risk analysis and mitigative action plan(s) for further escalation to the ET as appropriate, if broader impact identified

Breach Type	Severity / Materiality	Accountable Stakeholder	Reporting Group	Next Steps / Actions
Significant delays in proposed mitigation strategies	Proposed mitigation strategies are delayed / deferred	Risk Owner	ET and FAC	Prompt escalation to the immediate next reporting level with rationale(s) for the delay / deferral and an updated timeline for approval and for further escalation to the ET and FAC as appropriate

9. THE RISK MANAGEMENT PROCESS

Overview

Key to successful risk management is a structured process and approach. The process used at OMA aligns to ISO 31000. It will be applied for enterprise-wide risk management and can also be used for specific initiatives, projects, or activities.

The Process

The information below outlines the risk management steps.

Figure 2: Summary Risk Management Process

Specific steps within the process are outlined below.

Communication & Consultation

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

Establish the Scope, Context, Criteria

When establishing the context within its risk management process, the OMA will take into consideration the specifics of the current situation, internal and external environments – as well as the objectives of the ERM Program. The objective of the ERM program include the purpose, goals, and the key internal and external interfaces and 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.

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:

- ***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 OMA to consider the extent to which potential risks might have an impact on the achievement of strategic objectives. 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. OMA will utilize 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. OMA will use a Risk Register as the primary tool for articulating OMA's risk profile.

In evaluating risks for prioritization to drive further action, OMA will take into account the degree of control OMA 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 aggregate 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 cannot be reasonably mitigated by the OMA.

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 Executive Team will oversee the development and execution of risk treatments by the risk owner. It is not the intent in all cases to minimize, avoid or eliminate all risks that are identified, but more that OMA understand the significant risks that may negatively impact OMA and the stated strategic objective. 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
- ***Reduction*** – reducing the risk probability, consequence, or both
- ***Sharing*** – reducing risk probability or consequence by transferring or sharing a portion of the risk with a third party
- ***Acceptance*** – taking no action to affect probability or consequence

Monitoring & Review

Regular monitoring and review of risks are essential to understanding the changing dynamic of risk. The Executive Team will monitor risk management and update the risk information as applicable with input from Operational Excellence, ERM and the Risk Owners.

Recording & Reporting

Throughout the risk management process, the ERM Workgroup, Operational Excellence, ERM, Information Security & Technology Risk Office and the Executive Team 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 FAC and Board of Directors. Templates for reports can be found in the Risk Toolkit.

10. Reputation Management

Our reputation is important. OMA will consider and monitor events that might erode the trust of our members, staff, and Ontario's health care system, or impede our access to funding, reduce our stature with our key partners, cause widespread negative coverage or otherwise impact our reputation.

Every member of staff will be responsible for protecting OMA's credibility. The Executive team will be responsible for OMA's reputation management strategy and for the implementation of reputation management programs as this will require cross-functional efforts to enable a successful outcome. Management will raise risks and issues with potential to cause material reputation impacts to the FAC and Board as they arise.

Revision History

Author:	Operational Excellence, ERM
Process/Service Owner:	Chief Financial and Operating Officer
Approved by:	The Board

_____ _____

Signature (s) Date

Appendix A – Glossary

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

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

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

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

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

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 register: A tool used to facilitate prompt documentation, assessment, and reporting of risks that can threaten the achievement of the organization's objectives.

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

Risk treatment – process to modify risk

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

Appendix B - Three Lines of Defense and Roles & Responsibilities