OMA Ontario Medical Association

Effective Date: June 21, 2023
Next Review Date: June 21, 2025

Enterprise Risk Management Policy

1. PURPOSE

The purpose of the Enterprise Risk Management (ERM) Policy is to,

a) Articulate the Ontario Medical Association's (OMA[1]) approach to ERM and to provide an overview of the related roles, responsibilities, and accountabilities.
b) Establish and maintain a consistent, scalable approach to risk management throughout the OMA to support its mission, vision, strategic objectives, and governance.
c) Provide direction on the responsibilities and requirements of ERM to support the organization manage risks at all levels, enabling OMA leadership to take advantage of new opportunities, optimize the use of resources, and assist in the decision-making processes.
d) Integrate ERM as a common practice utilized by OMA across various sectors that aims to manage organizational risk necessary in the pursuit of strategic objectives, and that it forms part of the overall management system, helping to enhance the decision-making capabilities of management.

2. SCOPE

This Policy applies to all "*Users,*" including employees of the OMA, Board members, and OMA committee members.

3. PRINCIPLES

ERM is a continuous and active process at OMA that aids in the identification, understanding and management of the key risks that can have the greatest impact, either positively or negatively, on the achievement of our objectives.

This ERM Policy is in line with globally recognized standards: *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*.

[1] *OMA and its subsidiaries including Ontario Medical Association Insurance (OMAI), Ontario Medical Foundation (OMF) and OntarioMD are collectively referred to as "OMA" and / or "organization" throughout this ERM Policy.*

OMA is committed to fulfilling its mandate for managing risk and to support the achievement of organizational strategic goals and objectives by adopting the ERM principles. These principles are outlined in the ERM Framework.

4. ERM FRAMEWORK

The ERM Framework shall be used 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.

5. ERM GOVERNANCE

a) OMA has developed and instituted a robust governance structure to manage and oversee risks, and how risk roles and responsibilities are allocated across the organization. This includes the development and implementation of a risk governance structure that follows the Three Lines of Defense (LOD) model that is embedded within our existing organizational structure (*Attachment A*). It assigns clear ERM roles and responsibilities with appropriate independence and segregation of duties.

b) OMA shall comply with the OMA risk governance structure as set out in the Three LOD model described in the ERM Framework.

6. ERM STAKEHOLDER ROLES AND RESPONSILITIES

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 Finance and Audit Committee (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 Chief Financial and Operating Officer (CFOO), Executive Team (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.

7. 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 the organization. OMA adopts the Level 1 risk categories as identified and defined below:

Risk Taxonomy* (Level 1)	Definition
Strategic Risks	Risks that arise due to uncertainties from business decisions, implementation of business decisions or responsiveness to external changes.
Financial Risks	Risks that arise due to uncertainty surrounding the future investments / funds to meet OMA's investment goals.
Operational Risks	Risks that 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.
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.

** Refer to the ERM Framework for details on the OMA's Level 1 and 2 risk taxonomy.*

8. RISK APPETITE

The OMA's overall approach is to be a risk intelligent organization, all in the pursuit of our mission and role as an association to drive value for our members. In keeping consistent with this approach, the OMA shall articulate the organization's overarching risk appetite that is aligned and connected to its strategic goals to take the most appropriate risks in reaching its goals with the following considerations:

a) Risk Appetite Statements (RAS) articulate the amount of risk we are willing to take and/or accept in the pursuit of our objectives and to create value. Our strategy, direction and values inform its appetite for risk, along with other factors such as laws, regulations, and the broader operating environment. In turn, risk appetite sets a 'tone from the top' and helps inform our culture and decision-making process, assisting with establishing guidelines and boundaries within which risks shall be managed.

b) By integrating risk into our strategic and resources planning processes, and management system, we seek to optimize our risk returns. Our goal is to minimize negative exposures while accepting and encouraging an increased degree of calculated risk in pursuit of our mission and strategic objectives. We understand that our appetite for risk will vary according to the activity undertaken. Still, we strive to ensure that our approach to risk is systematic, consistent, that potential costs and benefits are considered, and that sensible measures to mitigate risks are established.

9. REPUTATIONAL RISK

Our reputation is of paramount importance. OMA is committed to considering and monitoring 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.

In this regard, we will consistently strive to mitigate risks to our reputation and to protect OMA's credibility by taking a systemic and cross-functional efforts to monitoring for possible events or situations that may potentially create degradation of OMA's reputation (including member and/or public confidence in OMA). We will concurrently prepare for unforeseen future events by having plans in place to effectively prevent situations from occurring while effectively mitigating situations as they arise to minimize adverse consequences to OMA's credibility and reputation.

10. 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 shall utilize both approaches in its ERM Program. The same core process shall be utilized for both regular cyclical assessment / management and as needed / ad hoc requests.

OMA shall implement and utilize regular reporting to effectively monitor and manage risks as set out in the OMA ERM Framework. This includes regular ERM cycle reporting, ad-hoc, confidential and time sensitive reporting.

11. ESCATION PROTOCOL

a) Operational Excellence, ERM shall escalate any changes in the following:
   - Material changes to the key risk profile
   - Significant delays in proposed mitigation strategies

b) Depending on the severity or the materiality of the change, the relevant information shall be reported to the Executive Team / Board to deliberate on next steps and action plans as per the escalation requirements set out in the ERM Framework.

12. POLICY EXPECTATIONS

The Policy establishes the following:

a) OMA implement risk management processes and periodically provide the management, the Board, and related stakeholders with an assessment of the effectiveness of these processes.
b) Risk management be integrated into strategic planning and resource allocation decisions.
c) OMA identify, analyze, evaluate, prioritize, treat, monitor, and report risks as an integral part of management and governance of resources.
d) Risk management activities comply with all applicable legal and regulatory requirements and consider industry leading practices.
e) Users manage risks effectively in their area of responsibility and identify and advise their manager or their department’s ERM Workgroup representative of potential risks.
f) OMA regularly reassess its risk ratings and the effectiveness of risk treatments in the context of the organization’s strategic objectives.
g) Operational Excellence, ERM be tasked with executing ERM at the OMA and ensuring risk information is consolidated and reported on a regular basis.
h) Managers and department leaders, with the aid of Operational Excellence, ERM review risks and associated information and provide regular reports to FAC.
i) Operational Excellence, ERM with the support of internal stakeholders, maintain department-level risk registers and an enterprise risk register, which include the identification, analysis, and evaluation of risks.
j) Operational Excellence, ERM plan and implement appropriate training to all employees, commensurate with their role within OMA’s ERM processes.
k) Operational Excellence, ERM collaborate and provide necessary information to OMA’s Internal Auditor to ensure the effective execution of respective duties.

13. COMPLIANCE

a) Compliance with this Policy is mandatory for all users.
b) Failures to follow this Policy may result in various remedial actions including, but not limited to, notification, additional training, coaching, and / or if applicable, interview with manager, Operational Excellence, ERM, relevant executive or People & Culture.

14. DEFINITIONS

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 organization from achieving its strategic priorities and supporting objectives, as well as positive risks that are in alignment with the organization’s strategic priorities and operational responsibilities.

Risk: Identified by ISO 31000 standard as the “effect of uncertainty on objectives.” In simple terms, a risk is the possibility of an event or a variable occurring with significance, affecting our goals, values, and the achievements of business strategies and objectives.

Risk Register: A tool used to document each identified risk and its related information. This includes the risks severity, responsible manager, lines of business affected, and summary of actions taken. It facilitates accountability and various insights and reporting.

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

Risk Appetite Statements (RAS): RAS express qualitatively the amount and type of risk(s) the organization is willing to take/ accept in pursuit of its strategic choices. RAS should be defined in the context of the strategic objectives as well as reflect risk preferences and ability of the organization to take and/ or accept risks.

Mitigation: Existing measures in place to mitigate the risk. It includes any process, policy, device, practice or other actions that reduces the likelihood and/or impact of the risk.

Three Lines of Defense (LOD): 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.

Risk Owner: The individual with the authority to ensure adequate mitigation strategies are in place to manage the risks they are responsible for and make additional recommendations to further manage those risks.

15. SUPPORTING/REFERENCED DOCUMENTS AND TEMPLATES

Use Type	Document Title
Mandatory	Information Security Policy Procurement and Contracts Policy Information Confidentiality Policy Privacy and Security Breach Management Policy and Procedure Whistleblower Policy
Supporting	Code of Conduct Policy Security Awareness Training Policy Coordinated Emergency Response Plan

	Social and Digital Media Policy Internal Electronic Communication Policy ERM Framework

16. RESPONSIBILITIES AND REVISION HISTORY

Position	Actions
Board (Approver)	Approves Operating Policies and/ or procedures.
CEO (Reviewer)	Reviews and recommends operating policies and/or procedures.
Author (Process / Service Owner)	Accountable for the service/process. Responsible for the design in alignment with the business objectives; and for the continual improvement of the service/process and supporting material.
Knowledge & Records	Review and provide additional metadata as required. Publish to OMA intranet (StaffSpace). Notify Authoring Department when each policy reaches its review date. Maintain original documentation for archiving.
Head of Departments	Monitor compliance with this policy and obtain training, if required.
Employees	Acknowledge as required and comply with policies/procedures.

Author: Operational Excellence, ERM

Process/Service Owner: Chief Financial and Operating Officer

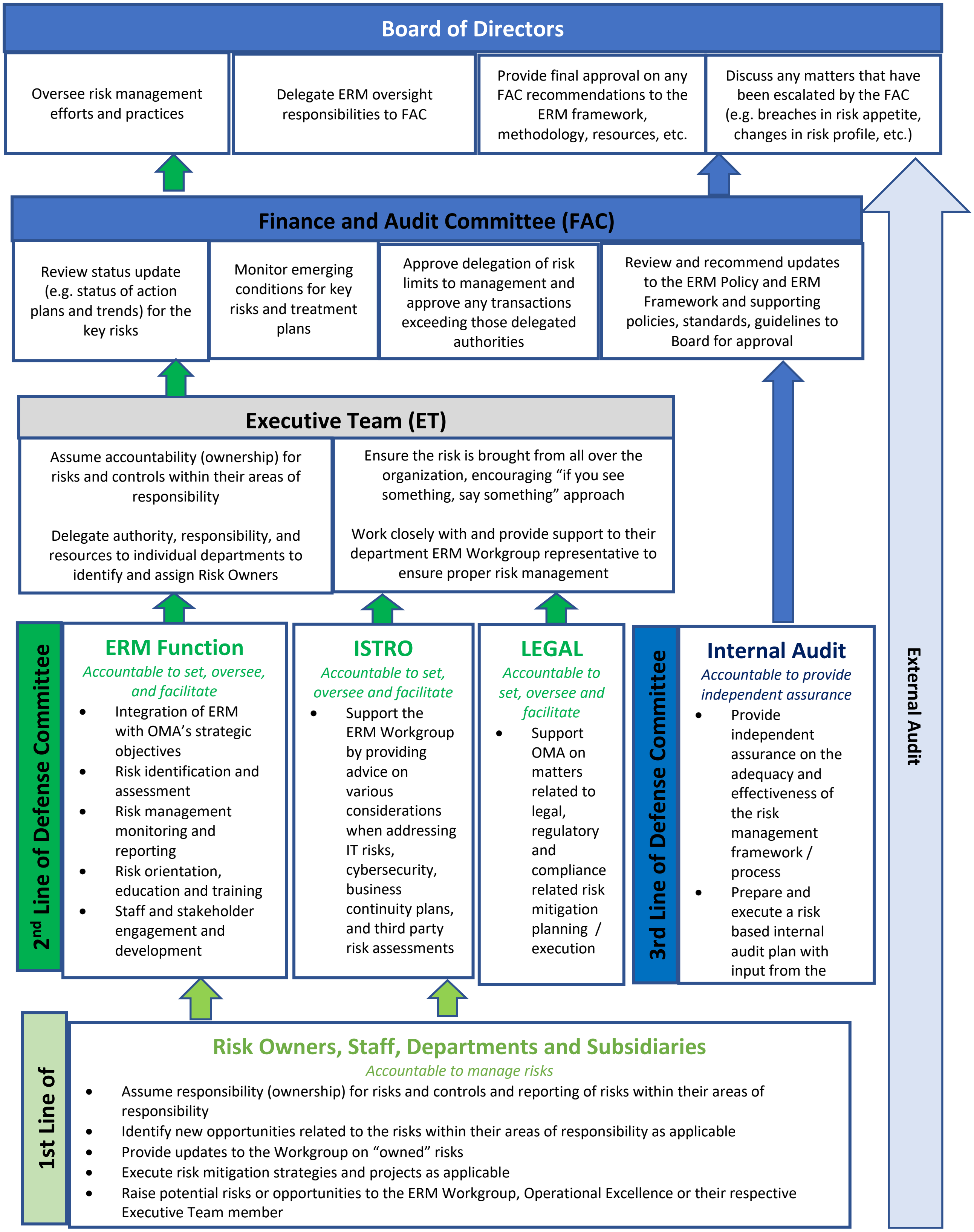
Approved by: The Board

OMA Board June 21, 2023

_________________________________ _________________________________

Signature (s) Date

APPENDIX A
Three Lines of Defense



Board of Directors

- Oversee risk management efforts and practices
- Delegate ERM oversight responsibilities to FAC
- Provide final approval on any FAC recommendations to the ERM framework, methodology, resources, etc.
- 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 status update (e.g. status of action plans and trends) for the key risks
- Monitor emerging conditions for key risks and treatment plans
- Approve delegation of risk limits to management and approve any transactions exceeding those delegated authorities
- Review and recommend updates to the ERM Policy and ERM Framework and supporting policies, standards, guidelines to Board for approval

Executive Team (ET)

Assume accountability (ownership) for risks and controls within their areas of responsibility

Delegate authority, responsibility, and resources to individual departments to identify and assign Risk Owners

Ensure the risk is brought from all over the organization, encouraging "if you see something, say something" approach

Work closely with and provide support to their department ERM Workgroup representative to ensure proper risk management

2nd Line of Defense Committee

ERM Function

Accountable to set, oversee, and facilitate

- Integration of ERM with OMA's strategic objectives
- Risk identification and assessment
- Risk management monitoring and reporting
- Risk orientation, education and training
- Staff and stakeholder engagement and development

ISTRO

Accountable to set, oversee and facilitate

- Support the ERM Workgroup by providing advice on various considerations when addressing IT risks, cybersecurity, business continuity plans, and third party risk assessments

LEGAL

Accountable to set, oversee and facilitate

- Support OMA on matters related to legal, regulatory and compliance related risk mitigation planning / execution

3rd Line of Defense Committee

Internal Audit

Accountable to provide independent assurance

- Provide independent assurance on the adequacy and effectiveness of the risk management framework / process
- Prepare and execute a risk based internal audit plan with input from the

External Audit

1st Line of

Risk Owners, Staff, Departments and Subsidiaries

Accountable to manage risks

- Assume responsibility (ownership) for risks and controls and reporting of risks 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
- Raise potential risks or opportunities to the ERM Workgroup, Operational Excellence or their respective Executive Team member