Enterprise Risk Management

1. Introduction

Sagility Limited (hereinafter referred to as "the Company" or "Sagility") is a technology-enabled healthcare focused solutions and services provider to Payers (Health insurance companies), and Providers (hospitals, physicians, and diagnostic and medical devices companies).

Sagility Limited defines risk in line with ISO 31000:2009 (Risk Management - Principles and Guidelines) as the "effect of uncertainty on objectives." Sagility faces various external and internal risks that could affect its financial and non-financial goals. To achieve its strategic objectives, the company prioritizes risk management to balance opportunities and risks, thereby protecting and enhancing stakeholder value.

1.1. Purpose and Objectives

The purpose of this policy is to establish a comprehensive Enterprise Risk Management (ERM) process that clearly defines the goals and responsibilities essential for effective risk management within the company and its group operations. It provides a structured framework for the Board to maintain oversight and control over risk management and compliance activities. This policy aims to ensure the Company proactively identifies, assesses, and manages risks amidst evolving business environments, thereby maintaining alignment with strategic objectives.

1.2. Regulatory Framework Requirements:

This Policy is based on the requirements of the Companies Act, 2013 and the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI LODR") as amended.

A. Requirements under Companies Act, 2013

- Section 134(3)(n) requires the Board of Directors, as part of the Board's Report, to give a statement indicating development and implementation of a risk management policy including identification therein of elements of risk, if any, which in their opinion, may threaten the existence of the company.
- The provisions of Section 177(4)(vii) require every Audit Committee to act in accordance with the terms of reference specified in writing by the Board which shall inter alia include evaluation of risk management systems.
- Code for Independent Directors Schedule IV requires Independent Directors to satisfy themselves that the systems of risk management are robust and defensible.

B. Requirements under SEBI (Listing obligations and Disclosure Requirements), as amended.

Role of the Board of Directors (Regulation 17)

- The Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan.
- The entity shall lay down procedures to inform members of the Board of Directors about risk assessment and minimization procedures.

Role of Audit Committee (Part C of Schedule II)

- The role of the Audit Committee shall include evaluation of risk management systems.

Risk Management Committee (Chapter IV)

- The Board of Directors shall constitute a Risk Management Committee.

- The Board of Directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit (such function shall specifically cover cyber security).

  The terms of reference for the Risk Management Committee under Regulation 21 are covered in Section 2.2 of this policy.

Corporate governance disclosures (Schedule V)

- The company shall include a comprehensive discussion on risks and concerns as part of the Management Discussion and Analysis section in the annual report.

- Corporate Governance Report shall include the following disclosures on Risk Management Committee
  - Brief description of terms of reference.
  - Composition, name of members and chairperson.
  - Meetings and attendance during the year.

1.3. Risk Management Guiding Principles

Sagility is committed to adhering to the following principles in pursuit of the objectives outlined in this policy. These guiding principles ensure a comprehensive, integrated approach to risk management that is embedded within the organizational culture and operations:

- **Shared Responsibility:** Risk management is the collective responsibility of every member of the organization, from the Board of Directors and Risk Management Committee to individual employees. Risks should be primarily managed by the business function transacting the business. All employees should actively engage in risk management within their own areas of responsibility.
- **Holistic Approach:** Sagility embraces a holistic risk management approach that seeks to optimize the balance between risk and return across all verticals and functions. By systematically evaluating and managing risks, the company ensures that only acceptable levels of risk are undertaken to achieve business objectives.
- **Continuous and Disciplined Process:** Risk management is a continuous, disciplined process that remains closely aligned with Sagility's approved risk appetite. This process is subject to ongoing refinement and improvement, ensuring it remains responsive to changing conditions and evolving best practices.
- **Adaptability and Evolution:** Sagility's risk management strategies are designed to be adaptive, evolving in line with international best practices and changes in requirements, organizational structure, size, and the industries within which the company operates. This ensures that the approach remains effective and relevant.
- **Comprehensive and Integrated Risk Management**: While ERM will serve as the umbrella function for addressing diverse risk aspects from strategic, operational, financial, and tactical perspectives, it will also synchronize with other risk-related functions. These include Internal Audit, Business Continuity Planning (BCP), Compliance, Information Security, Cyber Security etc. This collaboration ensures a cohesive strategy that effectively identifies, assesses, and mitigates risks across the entire organizational spectrum.

1.4. Scope of the Policy

The scope of the policy shall cover**:**

- Sagility Limited and its subsidiaries/ group companies.
- This policy shall apply consistently across levels of the Company, covering all operations, management, employees, contractors, business partners and/or individuals directly/ indirectly associated with Sagility.

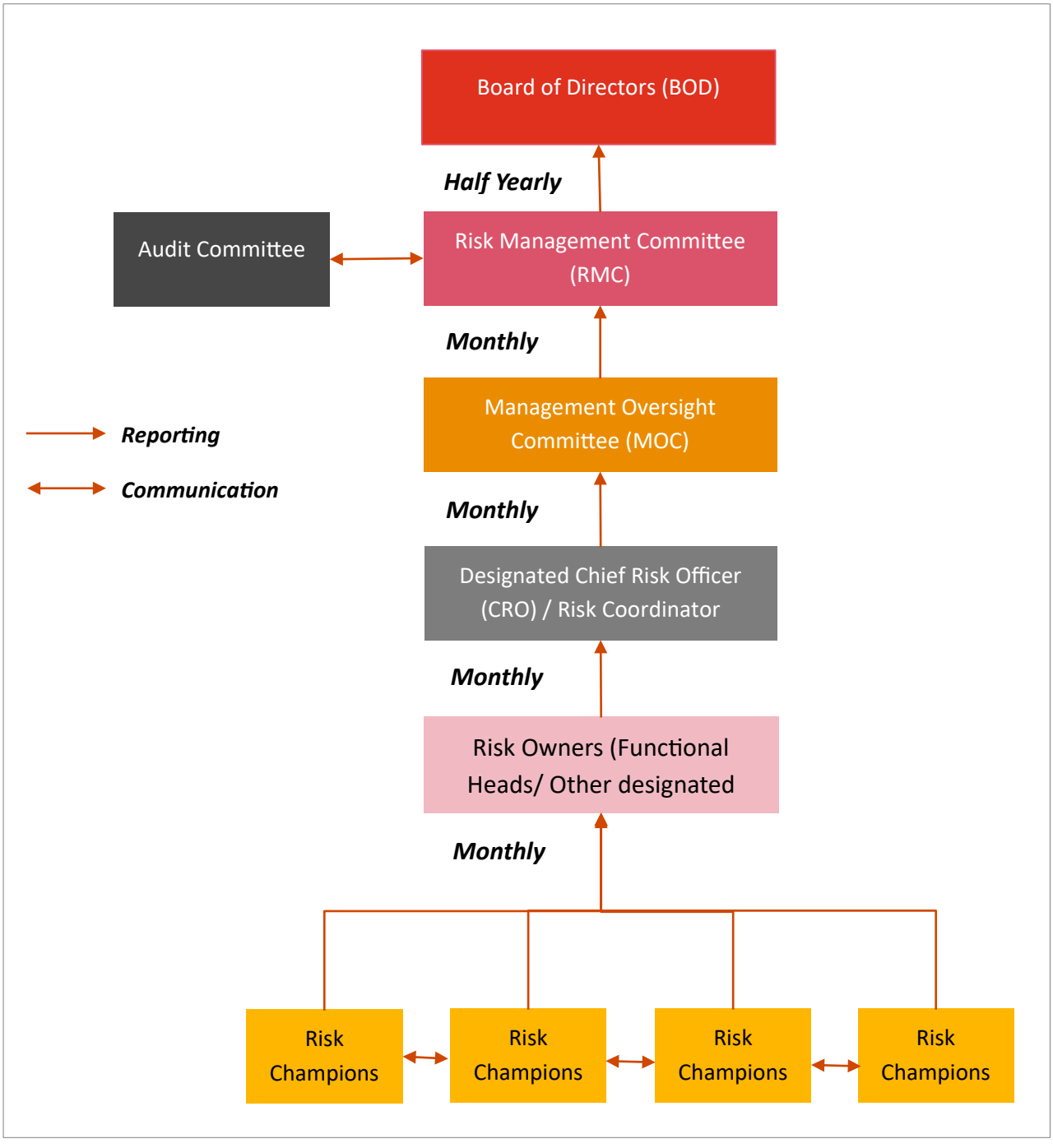
1.5. Review and Amendments

- This document will be reviewed by the Risk Management Committee (RMC) every two years, or more frequently if required by applicable regulations. Additionally, a review will be conducted in response to significant events, such as changes in organizational structure (e.g., entering or exiting a business segment), shifts in the risk profile, or alterations in government regulations. Any amendments to this policy will be subject to approval by the Board, following recommendations from the RMC.
- In the event of any conflict between the provisions of this Policy and The Companies Act, 2013 or SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("Applicable Law"), the provisions of the Applicable Law shall take precedence. Any amendments or modifications to the Applicable Law will automatically apply into this Policy.

2. Risk Governance Structure

2.1. Risk Management Organization Structure

A well-defined risk governance structure is essential for effectively communicating the organization's approach to risk management. It ensures a clear allocation of roles and responsibilities for managing risks on a daily basis. Sagility's risk management organizational structure is outlined below:



2.2. Risk Management Roles and Responsibilities

Roles and responsibilities for each member within the Risk Management organization structure are detailed below:

Roles	Terms of Reference
Board of Directors	Board is entrusted with the key role of ensuring effective risk management and aligning strategic objectives with the organization's key risks in order to achieve intended outcomes. • Implementation of this policy including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company. • Constitute Risk Management Committee is in line with applicable regulations. • Define the role and responsibility of the Risk Management Committee and delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit (such function shall specifically cover cyber security). • Review and approve risk management policy and amendments if any. • Ensure the integrity of the Company's systems for risk management. • End to end governance of ERM include effective implementation of the ERM framework and its regular monitoring. • Annually review and approve the Company's risk profile and risk appetite and evaluate the effectiveness of risk management procedures covering Key Risks and associated response plans. • Assist executive management by challenging the underlying assumptions: strategy, strategic initiatives (such as acquisitions), risk appetite, exposures and the key areas of focus.
Risk Management Committee	**Specific terms of reference as per the applicable regulations:** • RMC shall have a minimum of three members. • Majority of members to be members of the Board of Directors, • At least one independent director should be included in the Risk Management Committee (RMC). In the case of a listed company with special class equity shares labeled as 'SR', at least 2/3rd of the RMC must comprise independent directors. • The Chairperson of the RMC shall be a member of the Board of Directors and senior executives of the entity, may be additional members of the committee. CEO, CFO and Head of Internal Audit will be permanent invitees to the RMC. • RMC may invite other members who possess a range of relevant expertise as well as adequate knowledge, as selected by the committee members from time to time. • Quorum of the meeting to be 2 or 1/3rd of total members of RMC, whichever is higher, Including at least one member of Board in attendance. • The risk management committee shall meet at least twice a year. • The meetings of the RMC shall be conducted in such a manner that on a continuous basis, not more than 180 days shall elapse between any two consecutive meetings. Seek information from any employee, obtain outside legal or other professional advice and secure the attendance of outsiders with relevant expertise, if it is considered necessary.

Roles	Terms of Reference
	Roles and Responsibilities: • To facilitate management in formulating Risk Management policy which shall include**:** a. A framework for identification of internal and external risks faced by listed entities, including financial, operational, sectoral, sustainability (particularly Environment Sustainability and Governance -ESG -related risks), information, cybersecurity risks and any other risk determined by the RMC. b. Measures for risk mitigation including systems and processes for internal control of identified risks. c. A business continuity plan. • To ensure the implementation and oversight of risk management processes and systems that monitor, evaluate, and address risks associated with the Company's business, including assessing the adequacy of these systems. • To periodically review this policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity. • To keep the Board of Directors informed about the nature and content of its discussions, recommendations and actions to be taken. • Review appointment, removal and terms of remuneration of the CRO (if any) Coordinate activities with other committees (including MOC), where there is any overlap with the activities of such committees, as per the framework laid down by the Board of Directors. • Monitor and evaluate mitigation plans for key risks basis appropriate methodology, processes and systems. • Monitor the implementation of mitigation strategies for key risks and escalate to the Board and / or Audit Committee, as appropriate. • Integrate risk management Culture into the Organization.
Management Oversight Committee	MOC shall comprise of members from Finance, Technology, HR, Legal & Secretarial, Operations, Client Services, Sales & Marketing and additional invitees as nominated by MOC. **Roles and responsibilities** • Assess and evaluate the key risks anticipated and associated mitigation measures. • Ensure that effective risk mitigation plans are in place or recommend new mitigation measures as necessary. • Guide the risk owners in implementation of mitigation action. • Evaluate the early warning indicators “EWI” for key business risks identified by the risk owners. • Coordination with the RMC and CRO. • Ensure ownership of relevant risks is assigned to appropriate risk owners. • Provide inputs on emerging risks

Roles	Terms of Reference
Chief Risk Officer	CRO or equivalent personnel, as designated by Management, shall be the single point of contact / coordinator for risk management activities for the entire Company. **Roles and Responsibilities** • Manage and maintain the consolidated Enterprise Risk Repository. • Collate and review risk reports from the Risk Owners and prepare the consolidated risk report for Sagility for further presentation to MOC, RMC and the Board. • Act as Convenor in all MOC and RMC meetings. • Support the Risk Owners in identifying and assessing risks, creating mitigation plans, and development of Early Warning Indicators "EWI". • Assist in communication of inputs from MOC, RMC and the Board to respective risk owners. • Carry out any other activities with respect to risk management and oversight as may be delegated by the RMC and MOC.
Risk Owners	**Risk Owners** are Head of respective function/department/location or business leaders responsible for overseeing the management, monitoring, response, and emerging changes related to their assigned risks. They shall be the point of coordinating and managing all the risk management activities approved by the RMC and the Board. • Understand and take responsibility for the management of risk in their business units/functional areas. • Ensure that risks for their respective functions/department/location are identified and assessed. • Ensuring risk registers are maintained and updated on a monthly basis. • Ensure effective and efficient coverage of applicable risks. • Facilitate the identification and implementation of risk mitigation plans. • Track and measure the effectiveness of the mitigation plans. • Development of Early Warning Indicators "EWI's" for the identified risks to determine the occurrence of any risk scenario or event and monitoring the same • Reporting the risks along with assessment, mitigation plan and EWI status of their respective function to the CRO.
Risk Champion	**Risk Champions** shall be risk coordinators appointed by risk owners within their function (one or more than one) to assist in the risk management activities. • Assisting the Risk Owner in risk identification and assessments within their area of responsibility. • Taking timely input from the Risk Owners. • Compiling risks of the respective business vertical and reporting these to the Risk Owners. • Conduct a monthly update and review of the risk register for various functions, incorporating inputs from the Risk Owners. • Assist the Risk Owners in the development of mitigation plans and tracking of the EWI's.

3. Risk Management Process

The risk management process includes the following activities:

Activity	Description
Risk Identification	Identifying potential events or factors that could threaten the company's existence or significantly impact its operations. These risks may originate internally, such as through operations or strategies, or externally, due to market demands or regulatory changes. Various Categories of risks are as: **Categories of Risks:** • Strategic: Risks affecting high-level goals and alignment with the company's mission. • Operational: Risks impacting the effectiveness and efficiency of operations. • Financial: Risks affecting the company's performance and profitability, including safeguarding against financial losses. • Compliance: Risks related to adherence to laws and regulations. • Cyber Security/Information Technology: Risks affecting the integrity of networks, programs, technologies, and data. • Environment/Sustainability: Risks impacting operations, reputation, and financial performance due to environmental, social, or governance factors.
Risk Assessment	Evaluating risks based on their impact and probability to aid in prioritization.
Risk Prioritization	Ranking identified risks based on their impact and likelihood of occurrence. This process helps focus attention and resources on the most critical threats to a company's objectives.
Risk Mitigation	Addressing risks through specific strategies: • Risk Avoidance: Eliminating activities or conditions that lead to risks. • Risk Reduction: Minimizing risks' impact or likelihood when they cannot be avoided. • Risk Transfer: Passing the risk to external parties such as vendors or insurance firms. • Risk Acceptance: Choosing not to mitigate or reduce risks, accepting potential impact.
Risk Monitoring	Consistently review and evaluate risks to ensure that current mitigation strategies are effective and adjust plans as necessary for emerging risks. This involves tracking Early Warning Indicators (EWIs) to detect changes in risk exposure promptly.

4. Schedule and Responsibilities for Risk Management Activities

Roles	Maximum interval for meetings and activities		
	Periodicity as suggested by RMC	Half-Yearly *(There should not be more than 180 days gap between two consecutive meetings)*	Once in 2 years or in case of event requiring more frequent evaluation
Board	-	-	Approving the ERM Policy
Risk Management Committee	-	Review of the progress of ERM implementation Review the status of mitigation measures on the key risks	Review ERM Policy & process document for updates if any
Management Oversight Committee	Review and apprise RMC status for top risks and its mitigation. Discuss emerging risks	-	Review ERM Policy and process documents for updates if any
Risk Owners	Review Risk Register Reporting risks along with assessment and mitigation to the MOC	-	Provide input for updating of ERM Policy to MOC
Risk Champions	Identification of new risks and Updation of Risk Register	-	-

5. References

The Risk Management Committee (RMC) will provide detailed guidance on Enterprise Risk Management (ERM) activities within the Risk Management Framework document. This policy should be read in conjunction with the Risk Management Framework document.

6. Glossary

Term	Description
Board	Board of Directors
CFO	Chief Finance Officer
CRO	Chief Risk Officer
CDO	Chief Delivery Officer
CHRO	Chief Human Resource Officer
CISO	Chief Information Systems Officer
ERM	Enterprise Risk Management
CGO	Chief Growth Officer
ESG	Environmental, Social, and Governance
RMC	Risk Management Committee
MOC	Management Oversight Committee
BCP	Business Continuity Planning
COSO	Committee of Sponsoring Organizations
EWI	Early Warning Indicator

****