ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

Document ID:	ADHML -RM Policy
Version	V4.0
Effective Date for this version	03/09/2025
Document Classification	Restricted
Next Review Date	On or before 31/08/2026 (Review and reissue once in a year)

Document Version Control				
Version	**Date**	**Created / Updated By**	**Reviewed By**	**Approved By**
1	1st July, 2018	Group Internal Audit	Executive Director and Group Head- Governance and Corporate Affairs	Audit and Risk Management Committee
2	15th July, 2021	Head of Risk Management	Executive Director and Group Head- Governance and Corporate Affairs	Risk Committee and Board of Directors
3	20th October, 2023	Head of Risk Management	Executive Director and Group Head- Governance and Corporate Affairs	Risk Committee and Board of Directors
4	30th June, 2025	Head of IA, Risk Management and Compliance	Executive Director and Head- Governance and Corporate Affairs	Risk Management Committee (03/09/2025)

Aster
We'll Treat You Well

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

Risk Management Policy Administration

This revised policy framework document is effective from 03rd September 2025 being the date of approval by the Risk Management Committee. This version reflects the recent changes made in the Risk Management Framework such as updation of the policy after the split between India and GCC (to focus on India Operations and related risks), alignment of this framework to the strategies of the organization (pillars of excellence) where the risks are materially aligned with the strategies of the company, benchmarking carried out with risk management policies of other companies, within same sector and others.

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

Contents

1. Background 4
2. Purpose and Objectives 5
3. Risk Definition 6
4. Scope 6
5. Policy Requirements 7
   - 5.1 Risk Management Organization 7
   - 5.2 Risk Governance 13
   - 5.3 Risk Categories and Definitions 14
   - 5.4 Risk and Compliance Policy Framework 17
   - 5.5 Risk Culture 17
   - 5.6 Risk Management Cycle 18
     - 5.6.1 Risk Identification 19
     - 5.6.2 Risk Analysis & Assessment 19
     - 5.6.3 Risk Action or Treatment 21
     - 5.6.4 Risk Monitoring 21
     - 5.6.5 Risk Communication & Reporting 22
     - 5.6.5 Risk Register 22
6. Appendix 23

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

1. Background

Risk is the effect of uncertainty on an expected result and every business, irrespective of the sector, is exposed to it. The ability to effectively identify and manage risk is a vital element of success for all parts of a Company's business.

Risk can neither be avoided nor eliminated completely. Indeed, without taking risk, no business can grow - "Peter Drucker".

Businesses operate in a dynamic environment. Changes in government policies, legislation, information technology, customer preferences, competitors' initiatives, financial markets, etc. are a few aspects which contribute to this ever-changing environment, a situation demanding a mechanism to proactively foresee, assess risks and design de-risking strategies to reduce the adverse impact of the risk on the company. Effective Risk Management ensures sustenance of the company, and everyone associated with it.

Aster DM Healthcare Limited **(Termed as 'Aster' or 'Company' in this document)** as part of its business operations, takes risks on behalf of **its stakeholders*** (internal and external). It generates shareholder value by selectively taking exposure to risks where the risk is adequately rewarded and can be appropriately quantified and managed to safeguard the company's ability to meet commitments to its stakeholders and customers, comply with regulations, and protect its reputation.

The Risk Management Policy **(RMP)** defines the requirements for monitoring and managing the risks to which the business is exposed. The objective of the policy is to have a documented Risk Management Strategy in place, which provides a framework for timely identification, assessment, evaluation, mitigation, review and communication of the risk categories on a periodic basis. This policy document also lays down the framework for taking informed business decisions integrated with risks towards minimizing the adverse consequences of risks on business objectives. This would promote a proactive approach in analysis, reporting and mitigation of key risks associated with the business to ensure a sustainable business growth.

Our Enterprise Risk Management **(ERM)** function enables the achievement of the Company's strategic objectives by timely identifying, assessing, mitigating, monitoring, and governing any risk or potential threat to these objectives.

The proactive and systematic identification of risks and defining the de-risking strategies (i.e. mitigation actions) enables the company to improve performance with effective and timely decision-making. Critical decisions are taken after careful consideration of the potential risks, de-risking strategies and the resultant residual risks.

**The Stakeholders encompass a wide range of individuals and groups who have a vested interest in the company's performance and actions. They include, however, not limited to shareholders, employees, consultants, customers, suppliers, creditors, the local community, regulatory bodies, and society at large.*

2. Purpose and Objectives

The RMP provides a disciplined and structured process for the overall management of risk. This is achieved through:

- Describing the company's approach to risk management (both top down and bottom-up approach) and the principles for taking and managing risk
- Outlining the governance structure by which the company operates
- Providing a common language and framework for managing all types of risk which is important for consistency and understanding the overall risk exposure
- Providing a reference point when considering risks, by defining and describing the company's risk appetite (as applicable), risk categorization, risk policies, risk culture and risk management cycle
- Promoting a responsible risk culture across the whole business, supported by the recruitment and training of individuals to ensure the capabilities and behaviors needed to develop and control the business are in place
- Outlining key processes for risk management and internal control that support compliance with relevant customer, statutory, regulatory and shareholder requirements
- Integrate Risk Management into the overall strategy of the company, so that the relevant risks are focused upon.

General Principles of Risk Management

- All risk management activities will be aligned to the company's objectives, strategies and priorities, and aims to protect and enhance the reputation and standing of the company. Currently, this is mapped / linked to the 7 pillars of the Excellence of the Company.
- Risk analysis will form part of the company's strategic planning, business planning and investment/project appraisal procedures.
- Risk management will be considered adequately on a risk-based approach to internal control, which is embedded in day-to-day operations of the company.
- The risk management approach will aim to gain an assurance on the reliability of company's systems and will form the key means by which the Board gains its direct assurance
- Personnel at all levels will have a responsibility to identify, evaluate and manage or report risks, and should be equipped to do so.
- The company will foster a culture, which provides for spreading best practice, lessons learnt, and expertise acquired from our risk management activities across the company for the benefit of the entire organization.

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

3. Risk Definition

Risk is an inherent aspect of the dynamic business environment. Risk is the probability of damage, liability, loss, or any other negative occurrence that can be caused by external or internal vulnerabilities, and that may be minimized through pre-emptive action. Risk arises on account of uncertainty of occurrence and unknown consequences if the risk event were to occur. The degree of uncertainty or likelihood of occurrence and impact of the risk outcome combined determines the **Gross magnitude** (exposure) of the risk. Gross magnitude adjusted with the effectiveness of the de-risking strategies will determine the **Net magnitude** (exposure) or the residual risk.

4. Scope

This policy applies to Aster DM Healthcare Limited and its subsidiaries having operations in India. This policy must be implemented across all units and functions, and each functional / unit head is responsible for ensuring that all areas under their responsibility appropriately adhere to and verify compliance with the policy requirements. RMP applies to the management of stakeholders* exposures across the company. In addition, it is the responsibility of the company's senior management to ensure full compliance with all local regulatory and statutory requirements.

In addition, the company adopts a dual approach to risk identification and management: a **top-down approach** to identify strategic risks at the Organizational / Enterprise level, and a **bottom-up approach** to capture operational (not covered in the strategic risk list) risks at business unit/ function level.

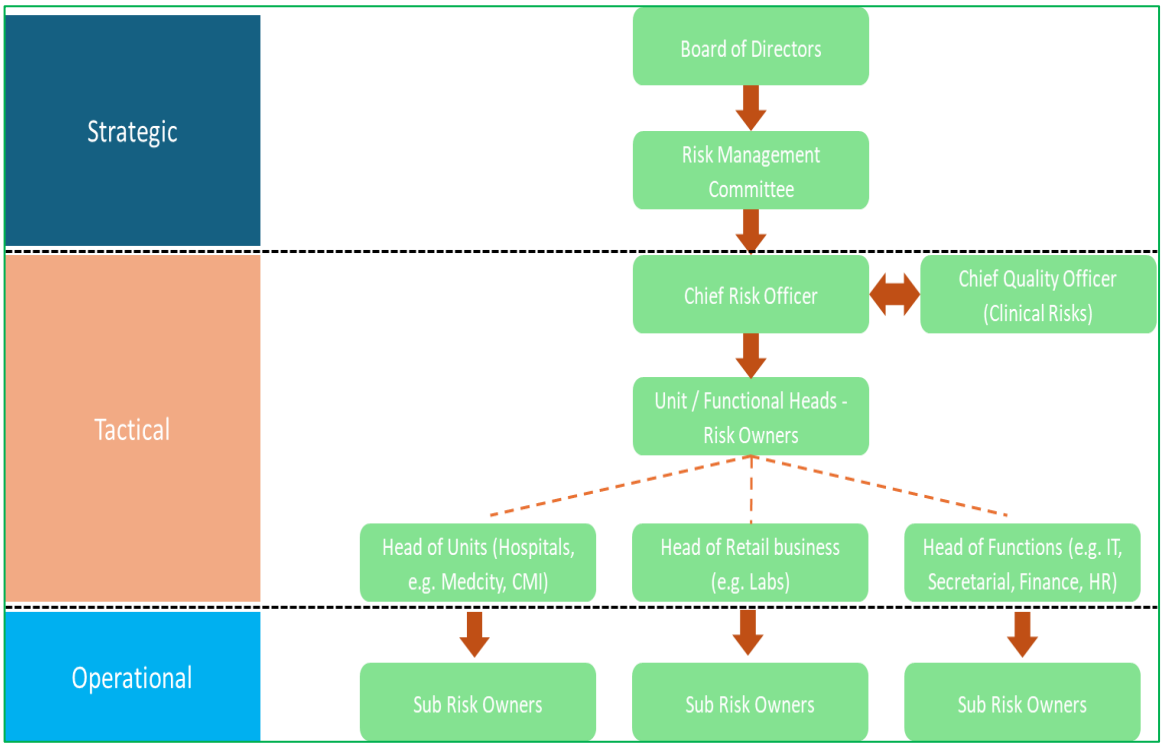
#	Activities	Enterprise level	Unit / Functional level
1	Overseeing by	Risk Management Committee	CXOs / Functional / Unit Heads
2	Nature of Risks Presented	Strategic Risks, which has an impact on overall Enterprise	Operational risks which is critical for the Function / Unit
3	Frequency	Quarterly	Quarterly

5. Policy Requirements

5.1 Risk Management Organization

Risk governance refers to the organizational structures, reporting relationships, delegation of authority, and roles and responsibilities that the company establishes to make decisions and control activities relating to risk management. It establishes oversight and challenge of the company's risk profile underpinned by risk policies and practices, risk appetite (if any), and the regulatory and statutory requirements. The Company's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities.

The Risk Organization Structure at an Enterprise level is provided below:



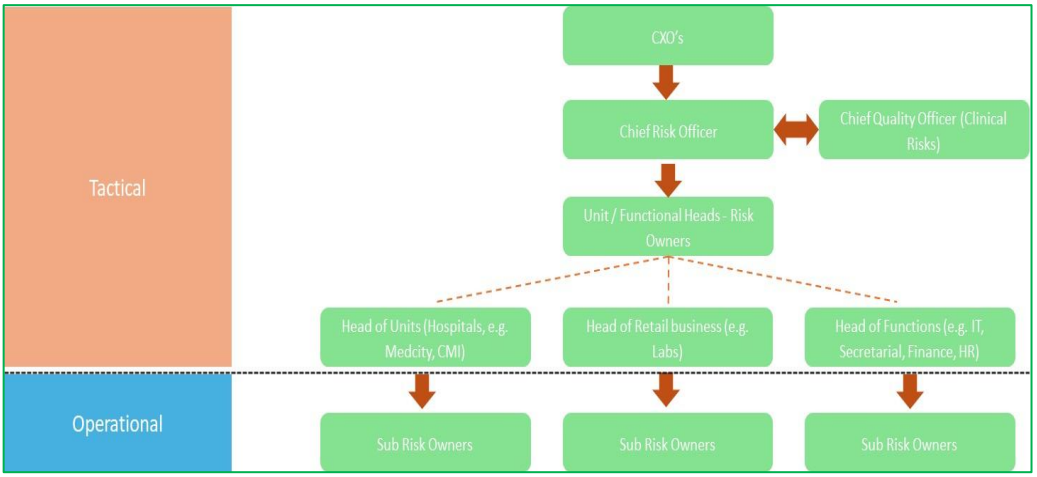
Notes:

1) The Medical Governance Committee is responsible for overseeing and monitoring clinical risks within the Company. The Committee focuses specifically on risks related to clinical care, patient safety, and medical staff performance. The Committee provides periodic input to the Board of Directors / RMC to support alignment between clinical practice and strategic governance
2) Chief Quality Officer monitors the Clinical risks and provides input to the Chief Risk Officer as appropriate
3) Technology Steering Committee is a committee, which oversees the IT / Technical / Digital related risks of the company and provides their inputs to Risk Committee / Board of Directors

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

The Risk Organization Structure at a Unit / Functional level is provided below:



Role	Definition
Board of Directors	• The board of directors shall ensure that the organization has proper risk management framework • The board of directors shall oversee the risk management plan for the company. • Understand the extent to which management has established effective enterprise risk management of the organization and the same is complied with all regulatory and statutory requirements as applicable • The board of directors shall define the role and responsibility of the Risk Management Committee as well as other Committees as applicable for the purpose of effective risk management • Be apprised by the Risk Management Committee and or Technology Steering Committee of the most significant risks and whether management is responding appropriately against such risks • Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks.
Risk Management Committee	• Risk Management Committee is the committee formed by the board of directors to oversee the risk management policy and risk management framework of the business • Formulate/amend risk management policy which shall include: (a) A framework for identification of internal and external risks of the Company, including financial, operational, sectoral, strategic, reputational, sustainability (including, ESG), information, cyber security risks or any other risk as may be determined by the Committee

	(b) Measures for de-risking, including systems and processes for internal control of identified risks (c) Business continuity and Disaster Recovery plan • Periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity and recommend for any amendment or modification thereof, as necessary to monitor and oversee implementation of the risk management policy • Policies and procedures establishing risk management governance, risk management procedures, and risk control infrastructure for operations. • Review significant reports from regulatory agencies relating to risk management and compliance issues, and management's responses • Provide advice and assurance to the Board of Directors by adopting a holistic and enterprise-wide view of the company and the key risks that it is exposed to, assessing the adequacy and effectiveness of the company's adoption of the Enterprise-Wide Risk Management Framework. • Keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken • Consider and review the prevailing risk culture in the organization (values, beliefs, knowledge, attitudes and understanding about risk) and maintain oversight of relevant work streams and projects to bring about the desired risk culture. • Review the risk identification and management process developed by management to confirm it is consistent with the Company's strategy and business plan. • To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company. • Oversee and monitor management's documentation of the material risks that the Company faces and update as events change and risks shift. • Assess the steps management has implemented to manage and mitigate identifiable risks (i.e. de-risking strategies) • Evaluate and assess the adequacies of the Key Risk Indicators (KRI's) defined and used by the management and see whether appropriate changes are made to those KRI's on a timely basis. • The Committee shall coordinate its activities with the other Committees in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors. • The Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it is necessary.

Chief Risk Officer (CRO)	• Head of Internal Audit, Risk Management and Compliance is designated as the CRO. • The responsibility of CRO and its team include: ✓ To coordinate the meeting of Risk Management Committee (RMC) at least once in six months or any other lesser frequency as decided by the RMC. ✓ Periodic update to the Risk Management Policy and submit it to the Risk Management Committee for review ✓ Identification of new risks that might be applicable for the company and that could impair achievement of the strategies. ✓ Evaluation of the existing risks and see whether any changes shall be made in line with internal / external environmental factors ✓ Assist the Board, Committees and senior management to establish and communicate the organization's ERM objectives and direction ✓ Assist management with integrating risk management with the overall strategy (i.e., Aster's 7 pillars of Excellence) ✓ Facilitate enterprise-wide risk assessments, developing de-risking strategies where required, and monitoring key risks across the organization ✓ Monitoring the Key Risk Indicators (KRIs) defined against Key Risks on a continuous basis (at least quarterly). Update the KRI's in line with changes to the risk portfolio ✓ Work with business units to establish, maintain, and continuously improve risk management capabilities ✓ Implement appropriate risk reporting to the RMC and Senior management ✓ Enables effective alignment between the risk management process and internal audit and statutory compliance management processes ✓ Responsible for coordinating with respective risk owners. Based on the inputs from units / functions, the CRO will prepare the consolidated risk register. All key risks identified shall be documented in the Risk Register maintained by Chief Risk Officer ✓ Strategic (Key/ Critical) risks to be presented to the Risk Committee while Operational risks to be monitored at CXO / Unit / Functional head level ✓ To monitor the de-risking strategies for the risks identified in the consolidated/ unit / function level risk register ✓ Measures to improve risk culture across organization (e.g., Risk Workshops, E-learnings and Trainings, Roadshows)

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

Internal Audit Team	• Key responsibilities of Internal Audit Team relating to risk management shall include: ✓ Implement a risk-based approach to planning and executing the internal audit process across the company. ✓ Submission of the internal audit plan to the Audit Committee and obtain approvals ✓ Coordinate and monitor the internal audit activities carried out by the co-sourced internal audit partners ✓ Evaluating the adequacy and effectiveness of the systems of internal control, including risk management, governance and operational processes ✓ Reporting to management on its findings, and its recommendations to remedy shortcomings ✓ Monitoring progress against these recommendations, and verifying the implementation of decisions taken based on the recommendations ✓ Provide inputs to the Risk Management Team, as applicable which will help on effective risk assessment.
Technology Steering Committee	• This Committee will have similar roles and responsibilities of the Risk Management Committee, however focusing only on Information Technology, Cyber and Digital risks that could impact achievement of the strategy / objectives of the company. • Evaluating the risk profiling of such risks, de-risking strategy effectiveness and effectiveness of Disaster Recovery Strategy (from data perspective) shall be considered by the Committee
Medical Governance Committee	• The Medical Governance Committee plays a critical role in overseeing and improving the quality, safety, and standards of clinical care. It acts as a key governance body to ensure that all clinical activities are aligned with best practices, regulatory requirements • While the broader Risk Management Committee may handle enterprise-wide risk, the Medical Governance Committee focuses specifically on risks related to clinical care, patient safety, and medical staff performance
Risk Owners / Sub-Owners	• Risk Owners are responsible for identification (including taking ownership of the risks) and implement de-risking strategies relating to their respective areas. • Risk Owners shall present the new risks identified along with the proposed de-risking strategies to the Chief Risk Officer. • Identify any upcoming risks, evaluate the criticality of the risk and formulate the steps for de-risking • Periodic review of the Risk register pertaining to their unit / function, work in collaboration with the CRO for update of risk register

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

Company Secretary	• Ensure periodic Risk Management Committee meetings are conducted in line with the requirement of the ACT • MoM of the meetings shall be circulated as per statutory requirements

5.2 Risk Governance

Aster's attitude to risk can be summarized as follows:

"As a provider of medical and health care services, Aster recognizes that the managed acceptance of risk lies at the heart of the business. As a result, effective risk management capabilities represent a key source of competitive advantage for Aster.

By managed acceptance of risk, Aster seeks to generate shareholder value by selectively taking exposure to risks for which it is well compensated. Aster will additionally accept exposure to risks for which it is not directly compensated, where these are an inevitable by-product of its business activities. These risks will be reduced to the extent it is cost-effective to do so.

In general, Aster's control procedures and systems are designed to manage risk, rather than eliminate it. However, at certain times, there may also exist some risks for which Aster has no tolerance, and which are actively avoided. Examples include having insufficient resources to cover its outgoing cash-flows or failure to comply with relevant regulatory/ statutory requirements or failure to carry out Ethical conduct."

Aster's risk appetite and tolerance to take on risk is specified through Risk Appetite Statements (RAS) and limits that are aligned to, and reviewed with respect to, the business model. Risk appetite is the amount and type of risk the organization is willing to accept in pursuit of its business objectives.

The Risk appetite statements (RAS), and their associated Key Risk Indicators (KRIs) enable the Business units and the Boards and Risk Committees to monitor and assess the Company's performance against its appetite to take on risk. Where any strategic / Critical Risk is proposed to be accepted (towards achievement of the objectives or strategy), those shall be presented duly to the Risk Management Committee by the CRO along with the Risk Owner.

KRIs include a balance of both lead (predictive) and lag (retrospective) measures to enable proactive risk management. Lead indicators (E.g., Number of doctors overdue for re-credentialing), provide early warnings of potential risk exposure, allowing the organization to intervene before harm occurs. Lag indicators (E.g., Increase in number of patient complaints, medical errors) offer insight into historical risk performance and help evaluate the effectiveness of existing controls.

Each risk owner, in collaboration with the Risk Management Function, shall identify and monitor relevant lead and lag indicators for key risk areas. These indicators are regularly reviewed as part of risk reporting to the Risk Management Committee.

5.3 Risk Categories and Definitions

To ensure risks are effectively identified, assessed, and managed at the appropriate levels of the organization, all risks are classified as either Strategic / Critical or Operational (not covered in strategic risks) based on their nature, scope, and impact on organizational objectives.

Strategic risks, due to their **enterprise-wide implications**, complexity, and potential to impact long-term goals, financial sustainability, or reputation, are monitored and reviewed by the Risk Management Committee (RMC) and the Board of Directors. Risks which are critical can cut across any of the categories as defined below. **The strategic risks are consolidated, tracked and monitored in the Enterprise risk register**.

Strategic risks affect an organization's long-term goals and objectives. They can stem from poor financial planning, changes in market dynamics, competitive pressures, and shifts in customer preferences. The risk of loss for our business or failure to maximize decision-making opportunity resulting from ineffective, inefficient or inadequate senior management processes for the development and implementation of business strategy.

In contrast, **Operational risks (not covered in the strategic risk list)**, while critical to service delivery and process performance, are often localized and are best managed by those closest to the process - i.e., Department Heads, Functional Heads or Unit Heads. If needed only, these are also discussed / presented to the Risk Management Committee. **These operational risks are consolidated, tracked and monitored in Unit wise risk registers.**

Below is the list of various categories of risk that the company can face (not an exhaustive list)

#	Category	Pillars of Excellence to which the risk can be mainly mapped	Definition
1.	Compliance Risk	Brand Equity	The risk of financial or non-financial impact results from a failure to meet regulatory / statutory requirements or a failure to adequately consider regulatory / statutory expectations and standards. Such risks could be associated with healthcare licensing, accreditation as well as legal issues such as intellectual property.
2.	Financial Risk	Business Performance	The risk of loss or adverse change in the financial situation of the business or that of our customers, resulting from fluctuations in the level of market volatility, competition, costs associated with insurance, capital structure, credit and interest rate fluctuations, capital equipment, billing and revenue cycle management.

3.	Fraud Risk	Business Performance	The risk of failure to have adequate systems and controls in place to protect our business and its customers from internal and external frauds and comply with applicable legislation and regulations.
4.	Health and Safety Risk	Service and Clinical Excellence, Sustainability Risk	The risk of failure to have adequate systems and controls in place to protect the health and safety of our customers and employees and our inability to effectively respond and handle crisis and waste management.
5.	Healthcare Quality Risk	Service and Clinical Excellence	The risk of failure to have adequate controls in place to prevent interruptions in critical care, inadequate service and negligence from doctors, failure to follow evidence-based practice, medication errors, hospital-acquired conditions, clinical incidents and so on.
6.	Information and Cyber Security Risk (Incl. Data Privacy)	Technology Excellence	The risk of failure to have adequate systems and controls in place to protect the data privacy and secure the data of our customers, other confidential information whose leakage can lead to litigation or business loss / reputational impact. Cybersecurity risk refers to the possibility of financial loss, operational disruption, or reputational damage due to failures or breaches in digital systems. These risks can originate from external attackers, internal misconfigurations, software flaws, supply chain partners, or even human error.
7.	Operational Risk	Across all Pillars of Excellence (depending on criticality, will be considered for RMC)	The business of health care is the delivery of care that is safe, timely, effective and patient centered within diverse populations. Operational risks can be the financial or non-financial impact resulting from inadequate or failed internal or outsourced processes and controls, credentialing and staffing, documentation, chain of command and deviation from practice. can be defined as the risks of loss arising from improper implementation of processes, external issues (weather problems, government regulations, political and environmental pressures, etc.
8.	Reputational Risk	Brand Equity	The risk that Aster through its activities, behaviors, and/or communications does not meet stakeholders' expectations in ways which adversely impact trust and Aster's reputation- potentially leading to a decline in revenue, increased costs, the loss of key personnel and/or adverse regulatory reaction.
9.	Resource Risk	People Excellence	The risk of negative impact on quality and inability to meet business objectives due to insufficient employment retention programs, ineffective succession plans, delay in recruitment of the right skill set or ineffective performance

			management systems
10.	ESG Risks	Sustainability & Community Connect	Environmental risks pertain to how Aster impacts the environment. Social risks comprise of fair pay, safe working conditions, ensuring supplier engagement and viable practices, seeking to provide employees with human rights, advocating for diversity, equity, and inclusion, and protecting data within Aster. Governance risks aid in the success of business operations and handling various policies and general communication strategies aimed at improving transparency within Aster DM.
11.	Catastrophic Risk	Sustainability & Community Connect	Catastrophic risk means a high-impact and minimal-probability event that might cause extreme damage on a global or large scale, threatening the very existence of human life and modern civilization (e.g., Natural disasters, Man-made disasters like riot)
12.	Concentration Risk	Business Performance	Risk of too much dependency on any unit, person, stream of therapy, clinicians etc., for generation of revenue or management of processes
13.	Emerging Risk	Across all Pillars of Excellence	Emerging risk includes risk that are new, evolving, or have limited precedent but may materially affect strategic objectives or operational resilience. These risks often arise from external changes, such as technology, regulation, environment, or social trends, and may carry high levels of uncertainty and complexity. E.g. of such risks include Advancement of artificial intelligence in healthcare, changing regulatory landscapes (DPDP Act, Labour code), new disease outbreaks, climate-related disruptions, or geopolitical instability
14.	Mergers & Acquisitions (M&A)	Business Performance	M&A risk primarily includes the risk that a merger, acquisition, or strategic partnership may not achieve its intended objectives due to poor due diligence, misaligned cultures, financial overreach, operational disruption, or inadequate integration planning.

5.4 Risk and Compliance Policy Framework

Policies are high-level statements which provide guidance on how the business operates with the aim of ensuring consistency and efficiency in, and accountability of, business processes and controls, and assisting the business in meeting its legal and regulatory obligations.

A key element of the Risk management policy is the suite of risk and compliance policies that covers the key risk areas faced by the company and supports the framework to facilitate effective risk management. The scope of these risk and compliance policies covers all risks (as defined within Section 5.3). The policies set out specific requirements to be applied in the management of each risk type.

5.5 Risk Culture

The Risk culture is reflected in the values and behaviors Aster displays when managing risk. Aster works to promote a responsible risk culture in the following ways:

- By the leadership and behaviors demonstrated by the management
- By requiring individuals to take responsibility for managing risks
- By building skills and capabilities to support risk management
- By emphasizing the importance of risk management in business decisions

Approach

The Aster leadership promotes a responsible culture of risk management by emphasizing the importance of balancing risk with profitability and growth in decision making, while encouraging compliance with regulatory requirements and internal policies. As part of this, they encourage all employees / personnel to be risk-aware, speak up and raise risks, to promote open dialogue around risk and to take personal responsibility for identifying and helping to address risk issues.

The Leadership team refrains from conflicts of interest and are held accountable for the decisions they make, specifically how they considered risk when making those decisions.

Risk Culture Requirements

All units / functions must:

- Promote a responsible culture of risk management exemplified by the risk culture characteristics listed below and behaviors of the leadership teams including: -
  - ✓ Articulation by the senior management, which is visibly supported by the decisions they take, on the need for good risk management to realize long term value
  - ✓ Employees / personnel understanding and caring about their role in managing risks for Aster and for customers and stakeholders, they are aware of and openly discuss risks as a part of the way they

perform their role; and

- ✓ Risk takers inviting open discussion on the approach to the management of risk

- Identify and deploy adequate and appropriate skills and resources and promote ongoing training and development to build management capabilities that recognize the consideration of risk in decision making
- Include quantitative and/or qualitative risk management objectives in the performance evaluation, reward and compensation of relevant individuals
- Embed risk management into decision making across the units / functions and consider risk management as part of "business as usual".

5.6 Risk Management Cycle

The risk management cycle is the ongoing process of identifying, measuring, managing, monitoring, communicating and reporting the risks to which the business is exposed to.

Elements / Process involved in the Risk Management Cycle (Both at an Enterprise or at a Function / Unit level) is provided below

5.6.1 Risk Identification

Comprehensive risk identification using a well-structured systematic process is critical. Identification should include all risks whether or not they are under the control of the Company. Continuous monitoring of the processes is undertaken to identify risks to which Aster is currently exposed or could be exposed to in the future. Structured processes apply, with the risks identified being categorized according to those risk categories and definitions laid out in section **5.3 of this document.** Risk identification can happen in any of the following ways (not an exhaustive list):

- ✓ Regular monitoring of a range of indicators by the business units and CRO / team to confirm that all material risks are captured.
- ✓ Workshops with Subject Matter Experts (SMEs)
- ✓ Brainstorming sessions
- ✓ Occurrence of a loss event
- ✓ Risk identification processes embedded in key projects
- ✓ Updates / inputs from external environment (in case of any event that had triggered outside Aster)
- ✓ Any Governmental policy changes, which potentially can impact the company

The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, or delay the achievement of objectives. Comprehensive risk identification is critical, because a risk that is not identified at this stage will not be included in further analysis. All identified risks should be updated in a risk register.

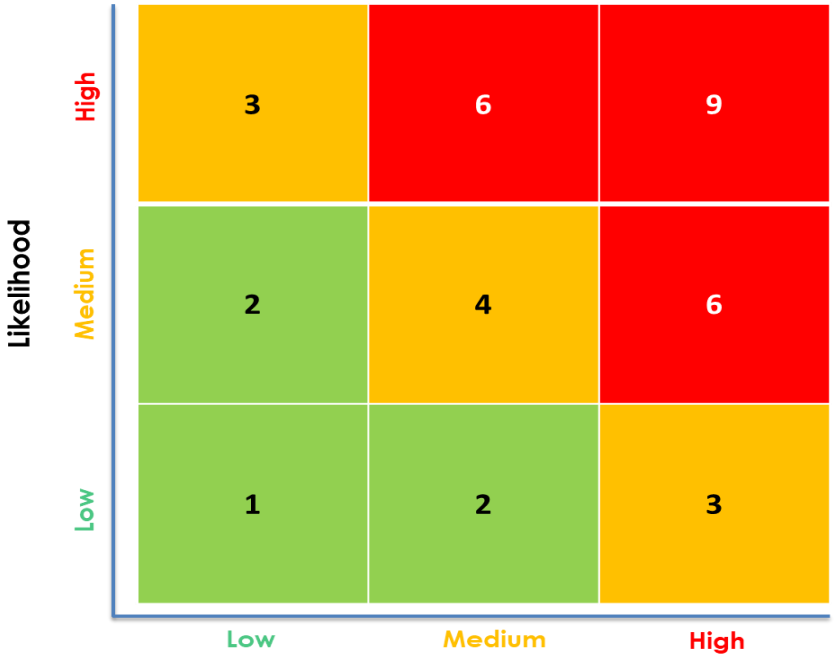
5.6.2 Risk Analysis & Assessment

Risks are measured using appropriate metrics as defined in setting risk limits, triggers and indicators. The risks will be assessed on qualitative two-fold criteria. The two components of risk assessment are

(a) the likelihood of the occurrence of the risk event and

(b) the magnitude of impact if the risk occurs. The combination of likelihood of occurrence and the magnitude of impact provides the inherent risk level. The magnitude of impact of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls.

Each risk owner shall arrive at a number of top risks for their function / departments. A three-by-three matrix shall be used for measuring likelihood and impact. A broad category of the gross / inherent risk rating using a combination of likelihood and impact is given below.



Significance of Impact

The magnitude of impact of a risk should it occur, and the likelihood of the risk occurring and its associated consequences may be determined using statistical analysis and calculations. Alternatively, where no past data is available, subjective estimates may be made which reflect an employee's or function / company's degree of belief that a particular event or outcome will occur.

In determining what constitutes a given level of risk the following scale is to be used for likelihood:

Level Descriptor

- 3 → High likelihood
- 2 → Moderate likelihood
- 1 → Low likelihood

In determining what constitutes a given level of risk the following scale is to be used for impact:

Level Descriptor

- 3 → High Impact
- 2 → Moderate Impact
- 1 → Low Impact

Likelihood and Impact product (Likelihood * Impact) can be considered as below

- 1, 2 → Low Risk

- 3, 4 and 5 → Moderate Risk
- 6 or above → High Risk

5.6.3 Risk Action or Treatment

Risk evaluation is the process to determine whether the risk and/ or its magnitude is acceptable or tolerable. Risk evaluation helps ensure appropriate resource allocation for the purpose of risk treatment and channelling of Management attention towards risks of significant concern. The prioritized risks must be compared with the risk appetite and all risks falling beyond the acceptable appetite must be shortlisted for risk treatment

Risk treatment involves definition of the de-risking strategies / controls for managing risks and implementing such re-risking strategies / actions. Individual risk profiles shall be prepared for the prioritized risks that shall serve as a descriptive record of each key risk. Details such as risk, risk owner, monitoring plans, timeline shall be maintained in the risk profile.

Various types of risk treatment are given below, which treatment to be selected shall depend on nature of the risks, risk appetite etc., of the company

- **Risk Avoidance:** If the risk assessment concludes that the risk is too high to be mitigated, it's possible to avoid the risk by resigning from performing specific actions or processes. The avoidance strategy is linked to interpreting the risk as unfavourable to the point that it should be excluded entirely. To avoid the risk, the company might choose to perform another action instead, as the alternative generates a lower threat.
- **Risk reduction / mitigation** is an important risk treatment strategy because it requires taking action to reduce the impact of a given risk while maximizing the benefits obtained from taking such action(s). To reduce the likelihood of risk or to bring its consequences down to an acceptable level, the company might implement safeguards or controls, carefully chosen from the range of available control processes.
- **Transferring risk** is related to passing a specific portion of the threat to another party to reduce its likelihood or impact on the company.
- **Risk Retention:** If the risk assessment concludes that the risk rating is at acceptable levels, or the mitigation cost of the implemented strategy is higher than the expected damage, the company might decide to accept the risk.

Once the effectiveness of the de-risking strategies gets applied to the relevant risks, the resultant would be the net exposure or residual risk exposure which the company will have.

5.6.4 Risk Monitoring

Risk monitoring shall be conducted by risk owners on a continuous basis, for identified risks, in order to analyze and track events, changes, and trends which affect identified risks. Further, detecting changes and assessing the impact of changes to risk appetite, risk portfolio, risk treatment plans and to ensure that risk treatment / mitigation mechanisms are effective in design and operation. This should also include monitoring the implementation and effectiveness of the de-risking strategies.

While operational (non-critical risks) shall be discussed with CXO's / Unit / Functional Heads, critical / strategic risks shall be presented to the Risk Management Committee.

Risk Control Matrix (RCM) maintained in accordance with Internal Finance Control (IFC) is an assurance process for internal financial controls documented in the form of risk matrices which enable the management and auditors to assess the design and operating effectiveness of the system of internal financial controls.

To be consistent with the Aster's Policy on Internal Audit and relevant standards / statutory requirements, Internal Audit team undertakes an annual risk-based planning process to determine the internal audit priorities for the year.

Appropriate documentation on each stage of the risk management process should be followed. The documentation will serve the following purposes:

- To demonstrate that the risk management process is conducted properly
- To provide evidence of a systematic approach to risk identification and analysis
- To provide a record of risks to support the development of a database of the Company's risks
- Provide responsible management with risk treatment plans for approval and subsequent implementation

5.6.5 Risk Communication & Reporting

Risk reporting and communication are important for the company to make informed risk management and resource allocation decisions. Risk communication is the process of communicating information about potential risks and uncertainties associated with a certain company's decision, action, or event.

Details of the Key Risk Indicators shall be included in risk communication and reporting, as these depict potential changes in risk exposure.

To ensure timely and appropriate decision making, the Board and Risk committee are provided with timely risk updates and management information. The main sources of reporting include:

- Communication on risk related matters between CRO, CXO's and Risk Owners is an ongoing process.
- Quarterly reporting to the Risk committee on strategic risks
- Monthly reporting to the CXO's / Unit / Functional Head on Operational risks
- Risk report on the Annual Financial Statements

5.6.5 Risk Register

- A risk register is a comprehensive document used to identify, assess, and prioritize potential risks in the risk management process. It provides a structured overview of risks, including their likelihood of occurrence, potential impact, risk owner details and de-risking strategies.
- Risk Register acts as a living document, which needs to be regularly updated in line with the evolving business and the external environment to ensure that all potential threats are accounted for and mitigated.

- Components of a Risk Register include the description of the risk, category of the risk, risk ownership, likelihood of occurrence, significance of impact, de-risking strategies, mitigation status of the risk etc.
- Risk owners are responsible for maintaining the risk registers (e.g. for a unit, the Unit Head would be responsible for) and updating them on a regular basis. CRO shall be responsible for having a consolidated risk register (both Enterprise and Unit / Function level). Any changes to the risk register shall be duly informed to the CRO.

6. Appendix

Reference to the Statutory Requirements (these could change, with any modification in the statutory requirement)

- Companies ACT, 2013 - Section 134
- Companies ACT, 2013 - Section 177
- Companies ACT, 2013 - Schedule IV of the Act
- Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

Other Reference is COSO Framework (Committee of Sponsoring Organization of the Treadway Commission), which provides guidance on Risk Management Framework of an organization.

The COSO Framework is built on five key principles:

- **Control Environment:** This principle emphasizes foundational elements crucial for a robust internal control environment, such as integrity, ethical values, an unbiased board of directors, competent personnel, and individual accountability.
- **Risk Assessment:** This involves identifying and handling risks to achieve organizational goals. It includes setting clear goals, analyzing risks, considering the potential for fraud, and assessing changes that can affect internal control effectiveness.
- **Control Activities:** These are measures to mitigate risks, including selecting and developing control measures, general controls over technology, and deploying control activities through policies and procedures.
- **Information and Communication:** Effective internal control relies on acquiring, using, and communicating relevant information. This ensures the quality and relevance of information used in decision-making and internal and external communication on control matters.
- **Monitoring Activities:** This involves ongoing reviews of internal control components to ensure effectiveness. It includes evaluations and timely communication of internal control deficiencies for corrective action.

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

For Sample of KRI's that is applicable at Enterprise Level or at Unit / Function Level Refer, Annexure 1 document

Glossary of Terms

Terminology	Description
Risk Management Committee	Risk Management Committee is the committee formed by the board of directors to oversee the risk management policy and global risk management framework of the business
Board of Directors / Board	As per Section 2(34) of the Companies Act (CA), 2013, a director is an individual who is appointed to the Board of the company. As per Section 2(10) of the CA Board or Board of Directors in the company means the altogether body of the directors of the company
Critical Risks	Risks identified as significant to the entity that if crystallized would seriously compromise Aster's ability to meet its strategic objectives or breach Risk Appetite Statement. Such risks need to be discussed / presented to the Risk Management Committee
Non-Critical Risks	Risks which can be monitored by CXO / Functional Heads / Unit Heads, however, might not be as critical from an overall company perspective. However, these risks could be critical at a functional / unit level. Such risks need not be presented to the Risk Management Committee
Risk	Risk is an event which can prevent, hinder and fail to further or otherwise obstruct the enterprise in achieving its objectives.
Inherent Risk / Gross Exposure	Is an assessed level of raw or untreated risk; that is, the natural level of risk inherent in a process or activity without doing anything to reduce the likelihood or mitigate the severity of a mishap, or the amount of risk before the application of the de-risking strategies

ASTER DM HEALTHCARE LIMITED (ADMHL)

RISK MANAGEMENT POLICY FRAMEWORK

Residual Risk / Net Exposure	Upon implementation of de-risking strategies, there will still be a degree of residual (or remaining) risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances. Thus, Residual risk is the threat that remains after all efforts to identify and eliminate risk have been made.
Risk Owner	Person / Entity with the accountability & authority to manage the risk is the Risk Owner
Emerging Risk	Newly developing or changing risks that are yet unclear in how they could impact the business and are therefore difficult to quantify (known, unknown). Emerging risks are typically issues that are perceived to be potentially significant, but which may not be fully understood, not yet quantifiable or not yet wholly reflected in the bottom-up risk assessments.
Risk Appetite	Risk appetite is the amount of risk that Aster is willing to take in pursuit of its strategic objectives.
Risk Profile	A risk profile is an overall evaluation of an individual or Company's risk and control environment.
Top of the House Risks	Top Risks are intended to provide a forward-looking view of the evolving risk profile, detail current risks meriting specific attention and those with the greatest potential impact on operating results and financial condition
Pillars of Excellence	7 Pillars of Excellence, which defines the strategy / vision of Aster *(People Excellence, Technology Excellence, Brand Equity, Service Excellence, Clinical Excellence, Business Performance, and Business Sustainability + Community Connect)*