AMRUTANJAN HEALTH CARE LIMITED

RISK MANAGEMENT POLICY

Risk Management Policy & Framework

1. **OBJECTIVES:**

The purpose of risk management is to identify, assess, mitigate, monitor the potential problems and report the before they occur, so that risk-control or mitigating activities may be planned and invoked as needed. This Policy also prescribes the risk management governance structure and framework and guides all internal stakeholders to manage adverse impacts on achieving the organizational objectives and in maintaining safety of assets & employees.

This policy establishes the process for the management of risks faced by Amrutanjan Health Care Limited (AHCL). The aim of risk management is to maximize favourable opportunities in all activities and to minimise adversity.

2. **SCOPE:**

This policy applies to all activities and processes associated with the normal operations of AHCL and includes events happening outside the Company but have a bearing on the company's business.

3. **DEFINITIONS:**

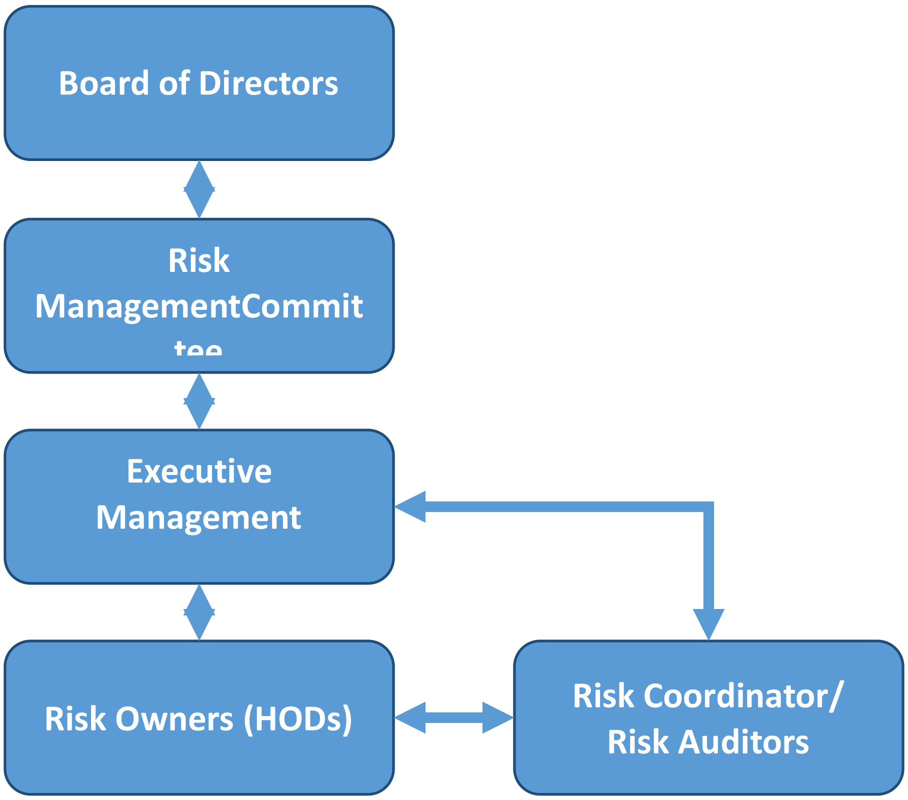
Risk: Risk is an event which can prevent, hinder and fail to further or otherwise obstruct the enterprise in achieving its objectives.

Inherent Risk: The risk that an activity would pose if no controls or other mitigating factors are in place (the gross risk or risk before controls).

Residual Risk: The amount of risk associated with an event or action remaining after the inherent risks have been reduced by risk controls.

Risk Appetite: Risk appetite is the amount risk, on a broad level, an organisation is willing to accept in pursuit of value.

4. RISK MANAGEMENT GOVERNANCE STRUCTURE



5. Risk Management Framework

Process Flow	Constituents
Policy & Framework	•Policy Statement •Framework •Risk Categories •Risk Appetite •Risk Evaluation Methodology
Procedure	•Reporting of Inherent Risks by Risk Owners (HOD) (Yearly) •Recording of Inherent Risks in the Risk Register (Yearly) •Auditing (Quarterly) •Reporting to RMC (Half yearly)
Documentation	•Risk Management Policy & Framework. •Risk Rating Criteria •Control Self-Assesment Questionnaire. •Risk Register. •Risk Audit Report • Risk Management Dashboard

6. POLICY STATEMENT:

The Risk Management Framework of AHCL is committed

- To achieve the organisational objectives by managing the associated risks through an integrated risk management plan;

- To ensure protection of stake holders value

- To provide clear fundamental principles for informed decision making at all levels of the organization

- To keep strengthening the Risk Management System by continuous learning & improvement

7. RISK ADMINISTRATION & RESPONSIBILITY:

7.1 Board of Directors (BOD):

The Board shall be responsible for defining the risk management strategy and objectives, overseeing the implementation of the risk management process and setting the tone and culture towards effective risk management. The board shall define the risk management policy and critically review the risk governance and monitoring mechanism. The Board shall meet at least once in a year to review the top risks faced by the Company and the status of their mitigation plan. It will also, review the Risk Management policy at least once in two years.

7.2 Risk Management Committee (RMC):

The Board of Directors shall constitute a **Risk Management Committee (RMC**) consisting of Board & Non-board members to guide on strategic risks associated with the company and to provide procedures & guidelines to be followed in the risk management process throughout the Company. The Committee shall be headed by the **Chairman & Managing Director**. The terms of reference of the RMC shall be as per the Resolution passed by the Board of Directors from time to time.

RMC shall co-ordinate its activities with audit committee, in instances where there is any overlap with activities of audit committee, as per the framework laid down by the Board.

7.3 Business Heads and Heads of Departments (Executive Management):

All members of the Executive Management shall perform the role of **Risk Owners** with regard to their respective functional areas. Risk Owners shall identify the inherent risks and report the same through the **Control Self-Assessment Questionnaire**to the Internal Auditor/Risk Coordinator on an annual basis for further investigation and to update the **Risk Register** and for further action to mitigate or minimise the impact of such risks. Every employee of the company is expected and encouraged to perform a role in risk management for identification of risk until its mitigation or treatment. The final ownership of risk identification, monitoring and mitigation shall rest with the members of the Executive Management.

7.4 Risk Coordinator:

The Chairman & Managing Director (CMD) shall identify a Risk Coordinator who would be responsible for conducting internal risk review meetings, maintaining risk registers as per the risk management policy and suggesting best practices for strengthening the risk management process. The risk coordinator shall ensure that the risk management processes as defined in this policy are executed and shall coordinate the effort of various functions to deliver the consolidated view to the Management and RMC.

8. RISK MANAGEMENT FRAMEWORK:

8.1 Risk Identification: Risks are about incidences that, when triggered, cause problems. Risk identification can start with the source of problems, or with the problem itself. This is the initial stage of risk management plan where different sources of risks are identified and their impact, causes and potential consequences are recorded for further analysis. The purpose of this step is to generate a comprehensive list of risks in each process or function that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is also important to identify the risks associated with not pursuing a business opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

8.2 Risk Analysis: Risk analysis involves consideration of the causes and sources of risk, the trigger events which would lead to the occurrence of the risk, positive and negative consequences of the risk, and the likelihood that those consequences would occur. At this stage, the inherent risksare evaluated and assessed for their likelihood and consequences based on **Risk Evaluation Methodology**. Existing measures of controls to mitigate the risk and their efficiency are considered.

8.3 Risk evaluation or Risk Audit: The purpose of risk evaluation is to assist in making decisions based on the outcome of risk analysis and target residual risk. This stage would incorporate decision taken by management based on the wider context of risk and its impact on the organization, its benefit. Decision should be made based on legal, regulatory, and other statutory requirements.

8.4 Risk Treatment: The process is to ensure that the risks are treated by appropriate selection and implementation of measures to mitigate the risk. The treatment can be done by risk mitigation, risk avoidance, risk transferor risk absorption.

8.5 Recording: All Risk needs to be recorded in Risk Register and updated regularly based on new identified risk. The Risk Coordinator shall ensure that all departmental level risk is being documented in Risk register.

9. CATEGORIES OF RISKS IDENTIFIED FOR AHCL:

1	**Strategic Risk**	Powerful new Competitor entering the market, Shift in customer demand, new product failure, key position turnover, single vendor dependence, unpredictable monsoons, changes in government policy due to economic recession
2	**Market Risk**	Counterfeit(fake)products, non-availability of products due to transport strike, liquidity crisis, acute talent shortage
3	**Operational Risk**	Unexpected failure in day-to-day operations, Spike in key raw materials & packing materials, Interruption in supply chain, process failure, fire natural and safety
4	**Financial Risk**	Reduction in Collections, Contingent liability becomes absolute liability, Investment risk, unfavorable foreign exchange fluctuations,
5	**Compliance Risk**	New regulations, major non-compliance, and non-compoundable risks under applicable laws
6	**Cyber Risk**	Financial or reputational loss arising out of : failure of information technology systems, Data Ex-filtration, Contagious software, financial theft, Internet failure, Information system security failure (Network/End Point/Backup/Secured access/Communications)

7	**ESG Risk**	**Environmental:** Geophysical(earthquake/Tsunami) Climatic change, Waste and Natural resource deficiency, Non-compliance of pollution control norms, change in production process or product design to meet environment standards, Occupational Risk **Social:** Socio economic trends (wealth inequality/Poor educational standards, migration) Human capital (labour disputes & strikes/employee misconduct/failure to attract talent) Brand perception(fake news/negative media coverage/negative customer experience) Infectious disease (Corona/unknown emergent disease) **Governance** Litigation (Lawsuits) Product defects/failure/Innovation failure(R&D) Business model deficiencies(Technology)

10. BUSINESS CONTINUITY PLAN (BCP):

The Heads of Departments shall draw up a Business Continuity Plan in respect of their functional area to ensure that the business unit, division, or function shall operate with minimum or no disruption in the event of occurrence of any event or incident that threatens the normal operation of the unit or division or the business.

11. IDENTIFICATION,MONITORING & REVIEW:

Risks so identified are assessed to classify them as per the criticality for the business. This would enable prioritization of risks and decide the right risk management strategies appropriate for the different class of risks. Wherever, applicable and feasible, the risk appetite is also defined, and adequate internal controls are installed to ensure that the limits are adhered to.

The Internal Control processes, ISO 31000 compliance and internal audit plans shall be designed in such a way that they align with the risk management process as provided in this Policy framework. Expert advise or consultancy may be availed for strengthening the risk control mechanism.

At the end of the risk assessment and evaluation, the Risk Management Committee shall periodically review the effectiveness of the risk management framework and measure the risk management performance against the key risk indicators. It shall also periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context.

12. RISK AUDIT REPORTING:

The executive management shall have the risk audit conducted at periodical intervals by an internal or external Risk auditor. Key risk reporting in the form of **Risk Management Dashboard** on half yearly basis shall be made to the Risk Management Committee at its duly convened meeting.

APPENDIX

Risk Rating Criteria (Risk Appetite) Risk Rating Criteria AHCL.docx

Risk Evaluation Methodology / Format of Risk Register Amrutanjan Risk register -

Control Self-Assessment Questionnaire Control Self Assessment

Risk Management Dashboard Risk Dashboard.xlsx