Risk Management Policy

Table of Contents

1.Introduction

Solara Active Pharma Sciences Ltd (Solara) is a customer a customer-oriented API manufacturer, with a legacy of over three decades. Its mission is to be a customer centric organization delivering APIs of high quality. Owing to the dynamic nature of pharma sector, which is largely regulated and has significant geo-political impact, Solara is exposed to varying nature of risks emerging from economic environment and technology space among others. Solara recognizes that such events present both risk and opportunities for future growth. Solara strives to proactively seize opportunities that the market offers in order to achieve its strategic and business objectives. It is recognized that in doing so, Solara is exposed to a number of external and internal risks which may affect its financial and non-financial results. This creates the need for Enterprise Risk Management (ERM) system to ensure minimal effect of the risks on Solara. Further, the regulatory norms and guidelines such as Companies Act 2013, Listing Agreement etc. are increasingly advocating the implementation of an effective enterprise wide risk management process for entities. With this in perspective and to ensure reasonable assurance over the attainment of its business objectives, Solara has decided to adopt a holistic risk management policy so as to guide their risk management activities.

1.1 Objectives of the Policy

The objective of this policy is to ensure sustainable business growth with stability and to promote a pro-active approach in identifying, evaluating, reporting and managing risks associated with the business. In order to achieve the key business objectives, the policy establishes a structured and disciplined approach to Risk Management in order to manage risk related issues. The specific objectives of the Risk Management Policy are:

1. To enable visibility and oversight of Board on risk management system and material risk exposures of the company.
2. To ensure all risks across the organisation are identified and evaluated through standardized process and consolidated across the organisation to identify the key risks that matter to the organization to enable risk prioritization.
3. To ensure mitigation plans for key risk are agreed upon, assigned to risk owners and reviewed on a periodic basis
4. To ensure that risks are reported at all levels in the organisation as per their relevance and significance.
5. To ensure that risk governance structure is aligned with organisational structure and risk profile of the company with well-defined and delineated roles, responsibility and delegation of authority.
6. To enable transparency of risk management activities with respect to internal and external stakeholders.
7. To enable compliance to appropriate regulations, wherever applicable, through the adoption of leading practices.
8. Assist in safeguarding the value and reputation by avoiding unpleasant shocks and surprises.

1.2 Scope of the Policy

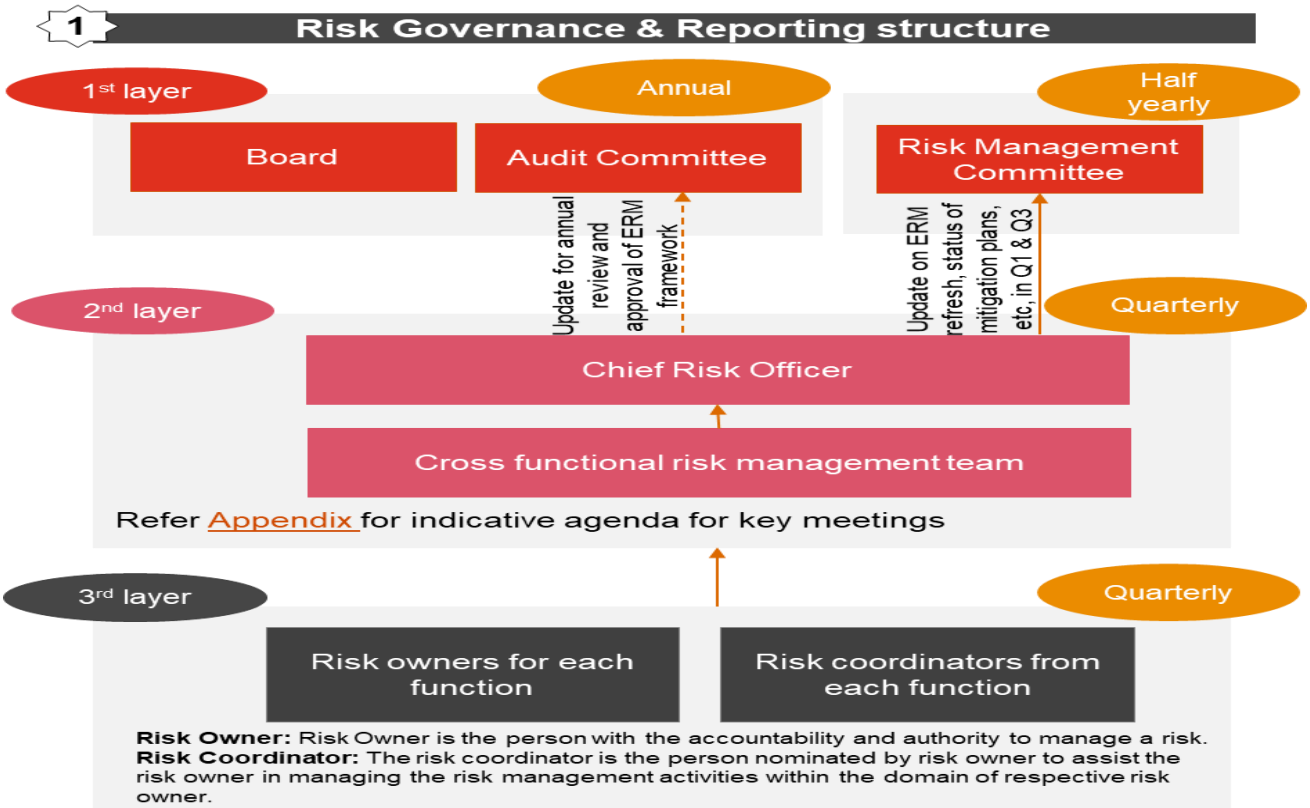
The policy guidelines are devised in context of the organization's growth objectives, its business and strategy plan, global ERM standards and leading ERM practices. The **Scope of the Policy** shall cover:

- All functions at corporate office
- All manufacturing divisions (plants) across the country
- All projects within India
- All events, both external and internal which shall have significant impact on the business objectives of the organization

2. *Risk Governance*

A well-defined risk governance structure serves to communicate the approach of risk management throughout the organisation by establishing clear allocation of roles and responsibilities for the management of risks on a day to day basis. In order to develop and implement an Enterprise Risk Management framework, SOLARA shall constitute a Cross Functional Risk Management Committee (CFRMC) which will ensure that risk management activities are undertaken as per the policy. Further to this, the main objective of the CFRMC shall be to provide an enterprise wide view of key risks within the organization to the Board. The CFRMC meetings shall be convened by CRO, who is responsible for establishment and implementation of risk management process effectively. CRO shall appoint Risk Owners from all relevant functions at SOLARA and Risk Owner would be responsible for establishment and implementation of risk management process effectively in their respective functions.

The diagram below outlines the governance structure for SOLARA:-



Note: The CRO shall be the convener for Cross Functional Risk Management Committee meetings and shall nominate the other members of the Cross Functional Risk Management Committee as and when the requirement for more departments' representation arises beyond the Management Committee in place at the time. The MD shall chair the CFRMC meetings.

2.1 Risk Governance Structure

2.1.1 Board

The Board is entrusted with the key role of ensuring effective risk management and aligning the strategic objectives with the organization's key risks in order to achieve intended outcomes.

Key roles and responsibilities

- Review and approval of risk management related guidelines and policy
- Ensure that risk management system is established, implemented and maintained in accordance with the defined framework

2.1.2 Cross Functional Risk Management Committee

Constitution of Cross Functional Risk Management Committee

The Cross Functional Risk Management Committee (CFRMC) shall constitute the CRO and Management Committee. The CRO shall be the convener for Cross Functional Risk Management Committee meetings and shall nominate the other members of the Cross Functional Risk Management Committee as and when the requirement for more departments' representation arises beyond the Management Committee in place at the time. The MD shall chair the CFRMC meetings.

Role and responsibilities of Cross Functional Risk Management Committee:

The Cross Functional Risk Management Committee shall have the key role of identifying the key risks, suggest mitigation measures, monitoring and supervising the implementation of the Risk Management Policy and maintain enterprise wide view of the key risks faced by the organization.

- Review the organization's risk profile periodically
- Review and assess the current & planned approach to manage key business risks
- Assess and evaluate the key risks anticipated and associated mitigation measures for the organization and suggest new mitigation measures as necessary.
- Ensure that effective risk mitigation plans are in place and the results are evaluated and acted upon.
- Report the key business risks faced by the organization and their mitigation plans to the Board
- In case of exigencies / emergent conditions, ensure that the Board is apprised about the same

2.1.3 Chief Risk Officer

The Chief Risk Officer (CRO) will work with members of CFRMC and Risk owners in establishing and implementation of risk management process effectively in their areas of responsibilities. The CRO shall be the convener of the CFRMC meetings. Further, CRO shall nominate additional members for CFRMC meetings as and when the requirement for more departments' representation arises.

Roles and Responsibilities of the CRO:

- Manage the establishment and ongoing maintenance of risk management policy pursuant to the organization's risk management vision.
- Ensure that the risk management priorities are reflected in the company's strategic plans and is considered during decision making

- Validate that the risk management policy is implemented in each department and that all significant risks are being recognized, acknowledged and effectively managed
- Discuss with risk owners and finalize the ownership of risk registers, thereby entrusting the person with the responsibility of completion of the risk register
- Coordinate with Risk Owners for periodic update of risk registers
- Definition of roles and responsibilities of Risk Management Panel (to operationalize risk management, also covering its composition (including KMP (Key Managerial Personnel), SMP (Senior Managerial Personnel) and CRO)
- Act as convener in RMC meetings and CFRMT meeting
- Periodic evaluation of risk environment and impact of changes in the ecosystem and discuss emerging risks during CFRMT meetings and update risk registers as needed
- Update RMC, Board and Audit committee on ERM adherence, emerging risks on a time to time basis (as indicated in the RM policy)
- Develop analytical, systems and data management capabilities to support the risk management framework.
- Measuring the organization's risk appetite, and setting the amount of risk that the organization is able and willing to take
- Monthly dashboards on risk mitigation status to be discussed in company's monthly review meeting, including metrics against defined KRIs
- Formulating and implementing risk assurance plans that are related to the transmission, storage and use of information and data systems
- Developing budgets for risk-related projects and supervising their funding
- Conducting risk assurance and due diligence on behalf of the organization in the event of mergers, acquisitions and business deal(s) taken up by the organization.
- Coach management teams in responding to risks.
- Monitor risk events and their impact both from global risks and local risks

2.1.4 Risk Owners

Risk Owners shall be the Heads of respective function/department/location as decided by CFRMC on time to time basis depending on the organisational structure and business imperatives so as to ensure that risks pertaining to all critical and significant functions/departments/locations are captured while identifying, assessing and managing risks. Their name shall reflect as the owner of the respective risk register.

Role and Responsibilities of Risk Owners:

Risk Owners should ensure that all the risks within their respective functions are identified, assessed, monitored and managed effectively to ensure that risk management practices are implemented. They should also ensure that processes utilized are in compliance with the entity's enterprise risk management policies.

- Ensure that risks for their respective functions/department/location are identified and assessed
- Ensuring that the risk assessment is done as per the risk assessment framework
- Ensuring risks are managed on a daily basis

- Ensuring risk registers are maintained and updated on a quarterly
- Facilitate the identification and implementation of risk mitigation and treatment plans as has been reviewed and approved by the CFRMC
- Reporting the risks along with assessment and mitigation of the respective function to the CRO

2.1.5 Risk Coordinators

Risk Coordinators shall be appointed by risk owners within their function (one or more than one) to assist in the risk management activities.

Role and Responsibilities of Risk Coordinators:

- Assisting the Risk Owner in initiating risk identification and assessments within their area of responsibility
- Taking timely inputs from Risk Owners
- Timely updating and maintaining the risk register for functions as per the inputs from Risk Owners.

2.2 Risk Reporting Structure

SOLARA shall have three line of risk reporting structure:

First Line of Reporting

- Risk Owners from each function and Risk co-ordinators shall report quarterly to Cross functional risk management team and CRO with all the risks identified in their respective functions.

Second Line of Reporting

- CRO shall convene Cross Functional Risk Management Committee meeting on a quarterly basis
- CRO shall consolidate the key risks based on the discussion of CFRMC which shall be reported to the Audit Committee for annual review and approval of ERM framework and to the Risk management committee on ERM refresh and Status of mitigation plan in Q1 and q3.

Third Line of Reporting

- CRO shall annually apprise the board on the key risks faced by the organization and the mitigation measures.

3. Risk Management Approach

Risk Management as a process shall enable the organization to identify, assess and treat risks. It is the responsibility of everyone in the organization viz. Board, Management Team and all SOLARA personnel. Risk Management applies to all functions, and operations within the organization.

In SOLARA, risk management is iterative. An iteration of the risk management process is triggered when e.g.:

- The business develops a new goal, undertakes a project or investment or considers its strategy for coming years

- Conditions exterior to SOLARA change significantly, e.g. regulatory or legal changes, major changes in competitive landscape, changes to key partnerships etc.
- Periodic requirements for risk reviews as required by Governing documents, Contracts, legislation or other sources

The primary objective(s) of establishing a Risk Management Process is to ensure that:

- Risks faced by the organization shall be identified and recorded in the risk register, enabling the top management to take a comprehensive view of the same

- Risks identified shall be assessed, mitigated, monitored and reviewed on an ongoing basis.

3.1 Risk Identification

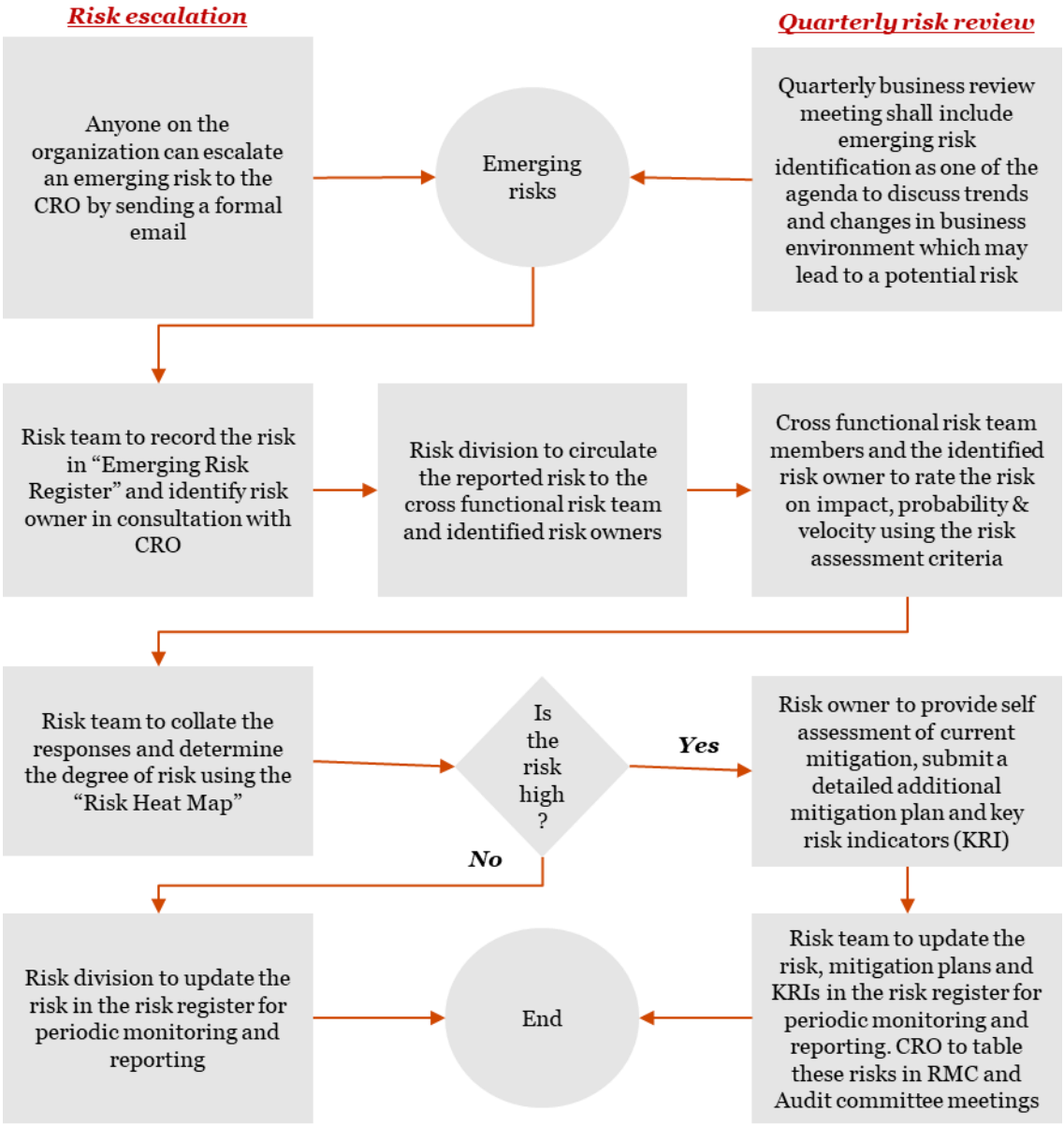
Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an in-depth knowledge of the organisation, the market in which it operates, the economic, legal, regulatory, social, political, technological and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification shall be approached in a methodical way to ensure that all significant activities within the organization have been identified and all the risks flowing from these activities defined.

The following methodologies can be used to identify risks:

- Brainstorming
- Surveys /Interviews/Working groups
- Experiential or Documented Knowledge
- Risk Lists - Lessons Learned
- Historical risk event information
- Please refer Annexure 1 for risk register template.

Emerging Risk



3.1.1 Risk Categorisation

All the risks that have been identified shall be categorised under the following risk categories - Strategic, Operational, Reporting and Compliance risk.

- **Strategic Risk** - Risk of loss resulting from business factors. These risks adversely affect the achievement of strategic objectives and may impair overall enterprise value.
- **Operational Risk** - Risk of loss resulting from inadequate or failed processes, people and information systems.
- **Financial Risk-** risk that a company won't be able to meet its obligations to pay back its debts. Which in turn could mean that potential investors will lose the money invested in the company.
- **Compliance Risk** - Risk of loss resulting from legal and regulatory factors

3.2 Risk Assessment

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management should assess events from two perspectives – likelihood and impact.

Risk rating is the result of the product of impact and likelihood of occurrence of a risk with the consideration of controls in place.

The risks identified will be evaluated by their likelihood and impact parameters as per the following methodology:

Parameters	1. Insignificant	2. Minor	3. Moderate	4. Major	5. Critical
Financial loss	Up to 0.2% of revenue	0.2% - 0.5% of revenue	0.5% - 1% of revenue	1% - 2% of revenue	More than 2% of revenue
Profitability – EBITDA	Less than 0.2% point impact on target EBITDA	0.2 - 0.3 % point impact on target EBITDA	0.3 - 0.5% point impact on target EBITDA	0.5 - 1% point impact on target EBITDA	More than 1% point impact on target EBITDA
Business suspension	1-2 days	3 - 7 days	8 - 30 days	1 - 3 months	More than 3 months
Reputation damage	Localized complaints	Repetitive public complaints	Negative local media coverage	Short term negative media coverage at national level	Continuous negative coverage at national & international level
Environment impact	Issue shared internally and response taken in-house	Internal situation (excess of regulatory limits)	Publicly known (leak to river/ lake, soil contamination)	Damage to business operations (Liability / physical damage)	Damage to fundamental business operations
Regulatory consequence	Insignificant or no impact	Minor compliance failures detected but waived / condoned	Warning show cause legal notice	Penalty up to INR 7.5 crores	- Penalty of INR 7.5 crores+ - Partial /complete prohibition of conducting business - Imprisonment
Customer satisfaction	Minimal complaints and recovery cost	Minimal or isolated impact on customer satisfaction	- Decline in customer satisfaction - Impact on sales	- Serious threat to future growth	- Wide-spread impact on customer satisfaction - Inability to sell
Operating conditions	Minimal change to work conditions	Short-term increase in working hours	Sustained deterioration in working conditions	Long term deterioration in working conditions resulting in increased sick	Unacceptable working conditions resulting in workplace injuries/ illness and resignations

In case, the rating based on different parameters are different, higher of the two or more ratings should be considered as the final risk rating.

E.g. For a particular risk, Impact rating is 3 based on the Compliance parameter and 2 based on the Premium parameter, the final impact rating should be taken to be as 3.

Estimate Likelihood of occurrence:

To assess the likelihood, the following classification matrix should be considered:

Rating	Significance	Past Occurrence	Future Occurrence
1	Unlikely	Once in more than 10 years	May occur in exceptional cases
2	Rare	Once in every 3-10 years	Unlikely to occur in next 3-10 years
3	Possible	Once in every 1-3 years	Likely to occur in next 1-3 years
4	Likely	Once in a year	Likely to occur in next 1 year
5	Almost Certain	Once in every 3 months	Likely to occur in next 3 months

Velocity

Rating	Significance	Velocity
1	Very slow	Impact of risk would be evident in 3 years and above
2	Slow	Impact of risk would be evident in 2-3 years
3	Medium	Impact of risk would be evident in 1-2 years
4	Rapid	Impact of risk would be evident in 3-12 months
5	Very rapid	Impact of risk would be evident in less than 3 months

Risk Exposure:

The risk assessment methodology adopted defines risk exposure as a product of Impact (rating) of the risk and the Likelihood of occurrence (rating) of the risk.

Weighted Average (Owner – 40%; Customer – 40%; Outsider – 20%)

Risk Criticality = Likelihood X Impact X Velocity

3.3 Risk Mitigation Strategy

There are four common strategies for treating risk. There is no single "best" response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

- **Risk avoidance/ termination:** This involves doing things differently and thus removing the risk (i.e. divestments). This is particularly important in terms of project risk, market risk or customer risk but often wishful thinking in terms of the strategic risks.

- **Risk reduction/ mitigation:** Reduce or Treat the risk. This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either:
    - Containment actions (lessen the likelihood or consequences and applied before the risk materializes) or;
    - Contingent actions (put into action after the risk has happened, i.e. reducing the impact. Must be pre-planned)

- **Risk acceptance/ retention:** Accept and tolerate the risk. Risk Management doesn't necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The organization shall tolerate such risks that are considered to be acceptable, for example:
    - a risk that cannot be mitigated cost effectively;
    - a risk that opens up greater benefits than loss
    - uncontrollable risks

It's the role of CFRMC to decide to tolerate a risk, and when such a decision is taken, the rationale behind it shall be fully documented. In addition, the risk shall continue to be monitored and contingency plans shall be in place in the event of the risk occurring.

- **Risk transfer:** Transfer some aspects of the risk to a third party. Examples of risk transfer include insurance and hedging. This option is particularly good for mitigating financial risks or risks to assets.
    a) The following aspects shall be considered for the transfer of identified risks to the transferring party:
        - Internal processes of the organization for managing and mitigating the identified risks.
        - Cost benefit of transferring the risk to the third party.

    b) Insurance can be used as one of the instrument for transferring risk.

3.3.1 Risk Reduction/ Mitigation Process

If the risk treatment mechanism selected is risk mitigation or risk transfer for an identified risk than the next step shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also identify new and improved controls.

Risk Mitigation Process:

Identify controls

New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite.

Control activities are categorized into Preventive or Detective on the basis of their nature and timing:

- Preventive controls – focus on preventing an error or irregularity.
- Detective controls – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

Implement Controls

It is the responsibility of the CFRMC to ensure that the risk mitigation plan for each function is in place and is reviewed regularly.

4. Risk Monitoring & Review

The Cross Functional Risk Management Committee is the key group which shall work on an ongoing basis within the risk management framework outlined in this policy to mitigate the risks to the organization's business as it may evolve over time.

4.1 Risk Monitoring

As the risk exposure of SOLARA may undergo change from time to time due to continuously changing environment, the risks with their mitigation measures shall be updated on a regular basis.

The following process shall be followed:

Quarterly

1. The risk owners and Risk Co-ordinators shall review and report the status of risks and treatment actions to the Cross functional risk management team and CRO.
2. Any new or changed risks shall be identified and escalated, if deemed necessary to the Chief Risk Officer (CRO).
3. The CRO with the other members of the CFRMC shall identify the key risks to be put up in the Board Meeting/Risk management committee/Audit Committee.
4. The CRO shall monitor and supervise the development and implementation of the Risk Management Policy and maintain enterprise wide view of the key risks and their mitigation measures undertaken by the organization.
5. The CRO shall report the key risks and their mitigation plans to the Board on annual basis.

Annually

1. The CRO shall annually report the key risks faced by the organization, their mitigation measures taken and the status of the risk management to the Board.

4.2 Risk Review

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified, assessed and appropriate controls are in place. Regular audits of policy and standards compliance shall be carried out and standards performance reviewed to identify opportunities for improvement. It shall be remembered that SOLARA operates in a dynamic environment. Changes in the organization and the environment in which it operates must be identified and appropriate modifications made to risk management practices. The monitoring process shall provide assurance that there are appropriate controls in place for the organization's risks.

The functional teams/risk owners shall review progress on the actions agreed to mitigate the risk and make an assessment of the current level of risk including:

- Establishing whether actions have been completed or are on target for completion.

- Report the status of implementation of mitigation plans to the CFRMC.

Any monitoring and review process shall also determine whether:

- The measures adopted resulted in what was intended.
- The procedures adopted and information gathered for undertaking the assessment was appropriate.
- The acceptability of each identified risk and their mitigation plan shall be assessed and risks shall then be ranked to identify key risks for the organization.
- Proposed actions to eliminate, reduce or manage each material risk shall be considered and agreed.
- Responsibilities for the mitigation measures for key risks management of each risk shall be assigned to appropriate functional heads.

5. Operation of Risk Management Policy

5.1 Approval of the Policy

The Board in their meeting held on 03.02.2021 has approved risk management policy. Further, Board has delegated authority and accountability to the Cross Functional Risk Management Committee constituting of Company's executive team. The Board shall maintain oversight over the activities of the committee and review it from time to time.

5.2 Review of the Policy

The risk management policy shall be reviewed as and when required but not later than 2 years based on changes in the business environment/ regulations/ standards/ best practices in the industry by an outside consultant/ organization that would present their recommendations to the Chief Risk Officer.

5.3 Maintenance of Risk Register

Centralized Risk register with their mitigation plan shall be maintained by CRO and shall be reviewed and updated as per the policy guidelines.

Annexure

Annexure 1: Format of Risk Register

S No.	Risk Sub - Category	Risk	Risk Description	Impact areas	Contextual information	Probability	Impact	Velocity	Risk score
1									
2									
3									
4									

Annexure 2: Definitions

Enterprise Risk Management

COSO's (Committee of Sponsoring Organisation of Treadway Commission) integrated framework defines ERM as:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Risk

One of the standard definitions of risk accepted worldwide in the domain of enterprise risk management has been framed by Committee of Sponsoring Organization of Treadway Commission (COSO) as a part of its 'Enterprise Risk Management – Integrated Framework' It defines risk as:

'*Risk is the possibility that an event will occur and adversely affect the achievement of objectives.*'

According to ISO 31000 standards, risk is the "*effect of uncertainty on objectives*" where an effect is a positive or negative deviation from what is expected.

In line with the above leading practices risk at Solara is defined as *'the possibility that an event will happen and adversely impact achievement of Solara's objective*'.

Risk Owner

Risk Owner is the person with the accountability and authority to manage a risk.

Risk Coordinator

The risk coordinator is the person nominated by risk owner to assist the risk owner in managing the risk management activities within the domain of respective risk owner.

Risk Identification

Risk identification is the process of identifying the organization's exposure to uncertainty.

Risk Assessment

Risk assessment is the overall process of risk analysis and risk evaluation. It allows an entity to consider the extent to which potential risk events have an impact on achievement of objectives.

Risk Treatment

Risk treatment determines the way to deal with risk. Various mechanisms to treat risk are:

I. Risk avoidance/ termination – decision not to become involved in, or action to withdraw from, a risk situation.

II. Risk transfer – sharing with another party the burden of loss or benefit or gain, for a risk.

III. Risk reduction/ mitigation – actions taken to lessen the probability, negative consequence, or both, associated with a risk.

IV. Risk acceptance/ retention – the acceptance of the burden of loss or benefit or gain, for a risk.

Risk Register

A 'Risk Register' is a document for recording the risks in a standardized format.