



RISK MANAGEMENT POLICY

Contents

1. Purpose	2
2. Objective.....	2
3. Scope & Applicability.....	3
4. Risk Management Framework.....	3
4.1 Risk Management Approach at GMM Pfaudler Limited.....	3
5. Risk Management Process.....	4
5.1 Identification and categorization of risks.....	4
5.2 Risk Description.....	5
5.2.1 Risk Documentation.....	6
5.3 Risk Rating.....	6
5.4 Identification of Risks That Matter (RTM).....	6
5.5 Risk Treatment Strategy.....	7
5.6 Monitoring of Risks.....	8
6. Risk Management Organization Structure.....	8
6.1 Roles and Responsibilities	9
6.1.1 Board of Directors.....	9
6.1.2 Risk Management Committee.....	9
6.1.3 Audit Committee.....	10
6.1.4 Chief Risk Officer.....	10
6.1.5 Executive Risk Management Council (ERMC).....	10
6.1.6 Risk Owners.....	11
6.1.7 Risk Champions.....	11
6.2 Risk Management Activity Calendar.....	11
6.3 Aligning Internal Audit with Enterprise Risk Management.....	11
7. Approval of the Policy.....	11
8. Review of the Policy.....	12

1. PURPOSE

The purpose of Risk Management policy is to ensure a sustainable growth of the organisation and to promote a pro-active approach in evaluating, mitigating and reporting risks associated with the business. Company is exposed to risks from strategic, regulatory, alliance, operational and financial perspectives. In order to achieve the purpose, the policy establishes a structured and disciplined approach to Risk Management in order to guide decisions on business risk issues.

The policy has been prepared pursuant to the following regulatory requirements:

- Companies Act 2013 requires that:
 - Section 134: The board of directors report must include a statement indicating development and implementation of a risk management policy for the company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the company. Audit Committee needs to evaluate the risk management system
 - Section 177: The audit committee shall act in accordance with the terms of reference specified in writing by the board, which shall, inter alia, include evaluation of risk management systems
 - Schedule IV: Independent directors should satisfy themselves that systems of risk management are robust and defensible
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 requires that:
 - Regulation 4 (2): Corporates to institute risk management framework comprising a process for risk assessment and minimization with roles and responsibilities for monitoring and reporting risks and controls.
 - Regulation 21: Broadly outlines the operating guidelines, powers and duties of the risk management committee

2. OBJECTIVE

The specific objectives of the Risk Management Policy are:

- To ensure that all the significant risk exposures, current and future, are identified, assessed, quantified, appropriately mitigated and managed
- To establish an operational framework for the risk management process and to ensure timely and adequate implementation
- To enable process to comply with appropriate regulations, wherever applicable, through the adoption of best practices
- To assure sustainable business growth with financial stability across business divisions

3. SCOPE & APPLICABILITY

- This policy is meant to ensure continuity of business and protection of interests of the investors and thus covers all the activities within the company and events outside the company which have a bearing on the company's business. The policy guidelines are devised in the context of:
 - the growth objectives, business profile envisaged and new business endeavours including new products and services that may be necessary to achieve these goals within the scope of review,
 - and adopting the emerging global standards and best practices amongst comparable organizations.
- The Risk Management Policy is applicable to all Businesses and Functions. Further, every employee of the company is recognized as having role in risk management for identification of risk to treatment and shall be invited & encouraged to participate in the process.

4. RISK MANAGEMENT FRAMEWORK

Risk management Framework is developed with an objective to enhance value of the Company and to the stakeholders (internal and external) by ensuring Company's business and growth objectives are protected. This framework facilitates decision making, planning and prioritization threats to business activities, fluctuations and balancing risks and opportunities. The framework is developed for enabling effective risk management, through consistent processes for risk identification, rating (assessment), treatment, and review and monitoring risks across the Company.

Through this framework, Company plans to inculcate a risk aware culture which will ensure that risk management is consistently practiced across the Company and highlight areas of focus for Management to make informed decisions to reduce the threats to the Company's business and growth objectives.

4.1 Risk Management Approach at GMM Pfaudler Limited

Company has adopted a comprehensive Enterprise Risk Management approach to identify and manage risks at an enterprise level. The risk methodology adopted is in line with leading Risk Management standard laid down by the Committee of Sponsoring Organizations (COSO).

The components of risk management are defined based Company's business and growth objectives, strategies, organizational structure, risk profile (categories and risk universe).

An effective Risk Management Framework comprises of:

- Risk management process: Risk management process has been divided into risk identification, risk rating and identification of Risks That Matter, Risk Treatment strategies and review and monitoring of risk management activities
- Risk management organization structure: The risk management processes will be supported the following:
 - Risk Management Organization Structure
 - Roles and Responsibilities
 - Risk management activity calendar
 - Frequency and mechanism for review the risk management policy

5. RISK MANAGEMENT PROCESS

The process of Risk Management shall cover the following:

1. **Risk Identification and Categorization** – Risk Identification is process of determining the potential events/threats that could prevent the Company from achieving its business and growth objectives. Based on their impact, these risks are categorised under broad categories of Strategic, Operational (SCM, People and IT), Financial and Compliance
 2. **Risk Description** – Involves systematic method of drafting Company's identified risks in a standard. It is important to record the risks as per the defined standard to help capture important aspects such as event, cause and effect in the statements
 3. **Risk Rating**– Process of rating the risks on predefined scales of impact and likelihood to assess the level of risks.
 4. **Identification of Risks That Matter (RTM)** – Based on the rating score of individual risks, Risks That Matter (RTM) are identified i.e. risks with the highest risk level are identified as RTM
 5. **Risk Treatment Strategy** – Risk treatment involves selecting one or more options for mitigating/modifying (reduce risk level) risks and implementing those options.
 6. **Monitoring of Risks** – Process of periodically monitoring the changes in risk and status of mitigation plan to assess the increase or decrease in risk rating.
- 5.1 Identification and categorization of risks
- Risk as defined by COSO is "the possibility that events will occur and affect the achievement of strategy and business objectives." Hence, risk identification can start with identification of source of risk event. This stage involves identification of risk events, areas of impacts, and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on events that impact (adverse or favourable) on achievement of objectives. It is important to identify the risks that may materialize in an event of loss of opportunities

It is critical that all the identification of risks is comprehensive as a risk that is not identified in this step will not be included in further analysis.

Categorization of risks

The risk profile of the company can be categorized as under:

- **Strategic Risks** are those that arise from the fundamental decisions that management/decision makers take concerning an organisation's objectives. Essentially, strategic risks are the risks of failing to achieve these business objectives. Other examples include business continuity, sustainability, failed mergers and acquisitions etc.
- **Operational Risk** are risks occurring due to inadequate or failed internal processes, people and systems, or from external events that cannot be controlled. Operational risks can be further classified in to
 - a. **Supply Chain Management (SCM):** Risks arising out of business partners (extended enterprises) such as vendors, subcontractors, fluctuations in commodity prices, aged inhouse production facilities etc.
 - b. **People:** Risks associated with Human Resources of the Company such as hiring and retention of the right talent, worker and labour management, attrition of key employees
 - c. **Information Technology:** Failure or disruption of systems, cyber-attacks, information security, loss of critical data management and integration of business applications
- **Financial Risk** is the possibility of financial losses, reduction in profitability of the Company. Some more common and distinct financial risks include working capital crunch, financial losses due to incorrect or no hedging etc.
- **Compliance Risk** are risks relating to non-compliance with regulations laid down by regulatory authorities in geographies of operations. Compliance risks will include legal, contractual and regulatory risks as well as code of conduct of the organization.

5.2 Risk Description

A risk description helps in ascertaining the details of a risk such as nature and quantum of risk and its likely impact and possible mitigation measures. Risk descriptions for each of the risks identified in the Risk Matrix may be documented and recorded in a structured format in each area where the risk is identified. Suggested structure of Risk Statement is as below:

[Event] that influences objectives caused by [cause/s] resulting in [consequence/s].

An alternative two statement version is:

[Event] that influences objectives caused by [cause/s]. This may result in [consequence/s].



The definitions for above terms are as below:

Event: is an occurrence or change of a particular set of circumstances/business environment and can have several causes.

Cause: is that which gives rise to any action, phenomenon, or condition. Generally, there are multiple causes and these are captured as contributing factors for each risk

Consequence: is the outcome (impact) of an event affecting objectives.

5.2.1 Risk Documentation

Risk statements from the Risk Description phase will be documented in a risk register. This risk register will be a central repository of risks of the organization and will cover important parameters such as risk statement, contributing factors, risk rating, risk level, mitigation plans, risk owners and risk champions

5.3 Risk Rating

Risk Rating Criteria is the first step for calculating the severity/level of a risk. Risk Rating assessment is based on the following:

Impact of the Risk on Company's Objectives and Goals: The degree of impact/consequences on the objectives of the Company should the event occur.

Likelihood of occurrence of the risk: The likelihood of the event is the probability/chances of occurrence of a risk event. Occurrence can be expressed as an annual frequency of occurrence of the risk event.

Risk Rating (Risk Score): Risk Rating or Risk Score is the product of Impact and Likelihood of a risk and is important to determine the risk levels

Risk Score = Risk Impact * Risk Likelihood

Risk Rating will be assigned jointly by all senior management personnel which would be part of Executive Risk Management Committee. Company has defined the rating scales and risk rating matrix basis the risk score assigned.

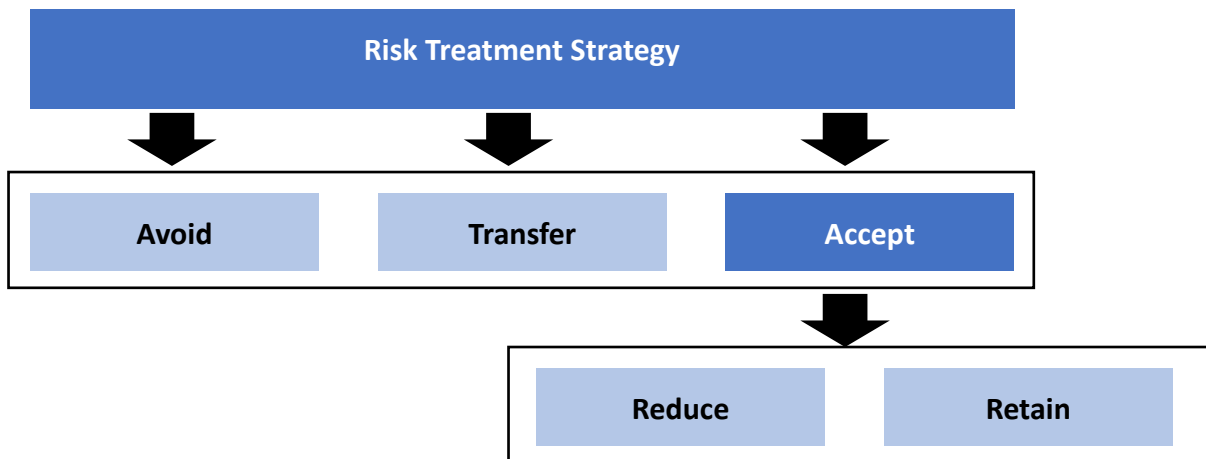
5.4 Identification of Risks That Matter (RTM)

Identification of Risks That Matter (RTM) is an extended activity of Risk Rating wherein, the risk score (Impact * Likelihood) of a risk is assessed. Post this, the top (say 8-10) risks with highest score are shortlisted and discussed with the management. On deliberation and feedback from the management, RTM are finalized.

Identification of RTM facilitates the management, risk owners and risk champions to focus on the main risks of the organization. Once these RTM are finalized, the management must develop the Risk Treatment Strategies

5.5 Risk Treatment Strategy

Risk Treatment is the process of selecting and implementing of mitigation plans to mitigate/modify (reduce the risk score) of risk. Based on Company's Risk Appetite, a Risk Treatment Strategy risk will be selected for each identified risk. The risk treatment strategy will include choosing from various risk treatment strategies. For Risks That Matter, Company may explore options of combination of two or more strategies. Following is the broad classification of Risk Treatment



Strategies:

- **Avoid (eliminate, withdraw from or not become involved):** Risk avoidance implies not to initiate or cease activities that are contributing factors of the risk. This strategy suggests implementing mitigation plans which eliminate or negate the possibility of occurrence of risk event to zero
- **Reduction (optimize/mitigate):** Risk reduction, optimization and/or mitigation involves reducing the severity of the impact or likelihood of occurrence. Acknowledging that risks can be downward or upward (opportunities), optimizing risks means finding a balance between downward risk and the benefit of the operation or activity poses.
- **Transfer (outsource or insure):** Risk transfer is a strategy that shifts risk from the Company to another party. A classic example of risk transfer is the purchase of an insurance. The risk is transferred from the Company to the insurance provider.
- **Retention (accept and budget):** Retention involves acceptance of risk event and loss upon materializing of the risk event. Risk retention is generally accepted for inherent risks of business where the cost of mitigation/transfer is greater than the impact of risk. All risks without a risk treatment plan involving the above three strategies are retained by default.

5.6 Monitoring of Risks

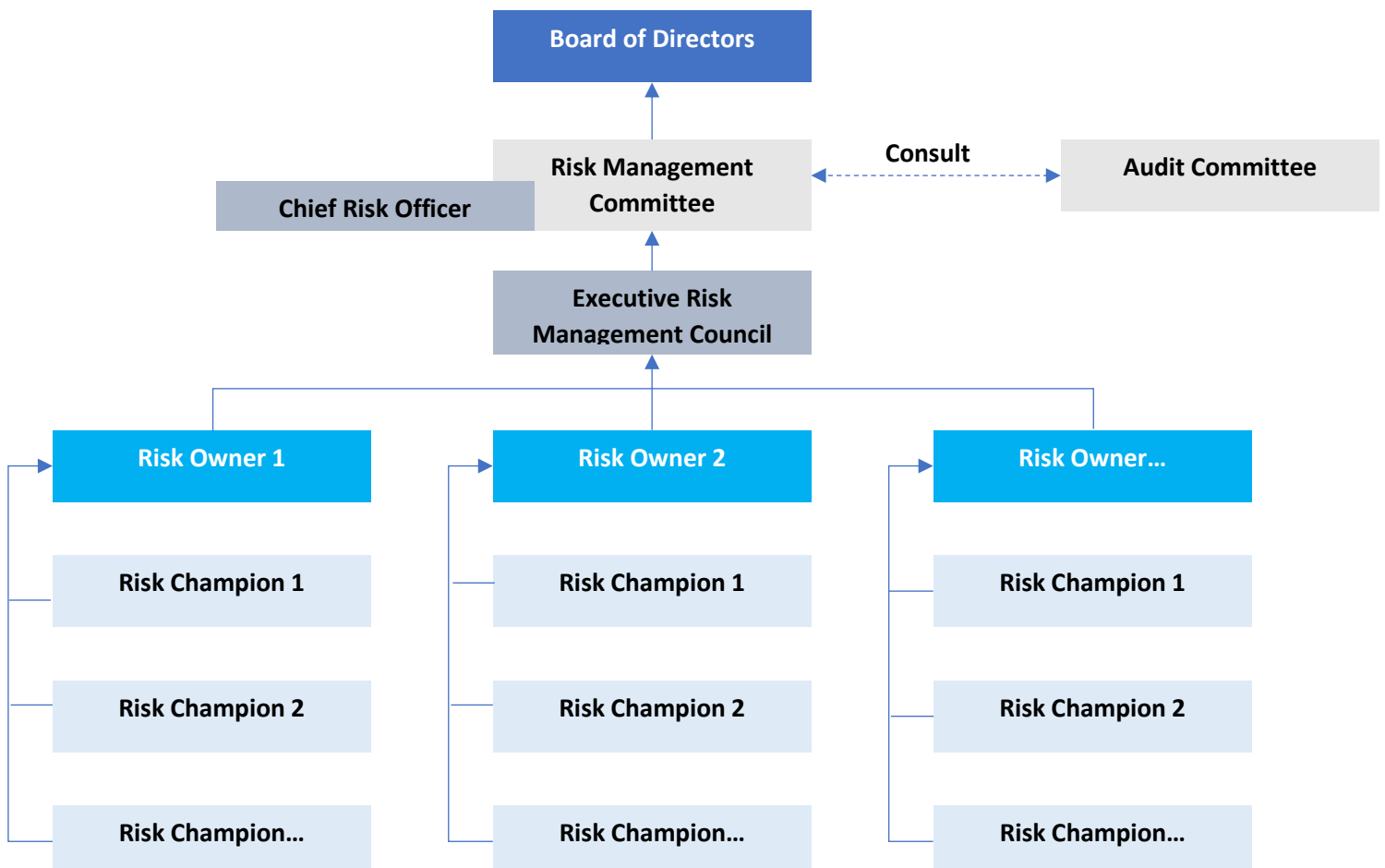
As the company grows and/or ventures in new segments and industries, risk exposure may undergo change. Hence, it is necessary to regularly review and update Risk Management documents as and when deemed necessary. The risk monitoring and review process will include:

- The CRO along with the support of Enterprise Risk Management Council (ERMC) will review the status of risks and risk mitigation plans with risk owners and champions.
- Any new or changed risks will be identified and escalated, if deemed necessary.
- It's important to focus on the high-risk areas and their action plans. The CRO will report collective findings to the Risk Management Committee at least on a biannual basis, or at a frequency mandated by the regulation.

All employees of the organisation are responsible for effective risk management. Management of the Company is responsible for ensuring development and implementation of risk mitigation plans and the risk management process will be integrated with the planning and reporting processes.

6. RISK MANAGEMENT ORGANIZATION STRUCTURE

Given below is the structure of the risk management organisation:



6.1 Roles and Responsibilities

6.1.1 Board of Directors

The Board, with assistance of Risk Management Committee will be responsible for supervision of risk management activities and implementation of an adequate tools for risk management across the Company. Board shall review the comprehensiveness and effectiveness of the Company's risk management activities on an annual basis.

6.1.2 Risk Management Committee

Roles and responsibilities

Following are broad responsibilities of the Risk Management Committee (as per the SEBI (LODR) (second amendments) vide notification No. SEBI/LAD-NRO/GN/2021/22 dated 5-May-2021):

- To formulate a detailed risk management policy which shall include:
 - Process of identification of risks with a specific focus on financial, operational, industry sector of Company and customers, sustainability (particularly ESG related risks), information and cyber security risks
 - Enablers for Risk mitigation via introduction tools and processes for internal control of identified risks.
 - Business continuity plan.
- To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks.
- Supervise and facilitate implementation of risk management policy and framework,
- To periodically review the risk management policy, at least once annually, considering the changing industry dynamics and regulatory requirements.
- Inform the Board about the evolving changes in the risk universe (landscape) and recommend actions to be taken

The Risk Management 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 considers necessary

Composition of Risk Management Committee

As per the revised SEBI regulations the Risk Management Committee shall have minimum three members with majority of them being members of Board of Directors, including at least one independent director.

6.1.3 Audit Committee

The Audit Committee would act as a consulting source to the Risk Management Committee and provide insights on risk management activities.

6.1.4 Chief Risk Officer

The Chief Risk Officer (CRO) will play an important role for the success of Company's Risk Management activities. CRO will work with the Risk Management Committee and will be a permanent invitee to all the Risk Management Committee meetings. CRO will be responsible for developing and implementing risk management policy and framework, review and monitoring of Risk Treatment strategies. The CRO will work closely with the Executive Risk Management Council (ERMC) and Risk Owners to identify risks and facilitate development of risk mitigation plans.

As the driver of Risk Management activities, the CRO will facilitate the execution of risk management processes and strengthen risk management infrastructure. Following are the key responsibilities of the CRO and CRO Office:

- Facilitate identification of new risks.
- Support the Board, RMC and Managing Director to establish and communicate the organization's ERM objectives
- Develop and communicate risk management policies.
- Facilitate risk management activities such as Risk Rating, developing Risk Treatment Plans and monitoring of Risk Management activities
- Assist in establishing, communicating and facilitate the use of appropriate ERM methodologies, tools and techniques
- Work with ERMC and Risk Owners to establish, maintain, and continuously improve risk management capabilities
- Enable effective alignment between the risk management process and internal audit

6.1.5 Executive Risk Management Council (ERMC)

- Members of ERMC will be the drivers of ERM process.
- Facilitate implementation of the ERM framework (in coordination with Risk Owners) and monitor timelines for risk management activities within the Company.
- Establish a process to consistently monitor business environment changes, threats and factors impacting the risk profile of the Company.
- Communicate internally and record new/change in risks (*as and when required*).
- Monitor progress of implementation of risk mitigation plans for Risks That Matter

Members of ERMC will be MD, CFO, CEO, Business Heads, Enabling Function Heads (HR, IT, other function heads).

6.1.6 Risk Owners

Risk Owners in consultation with Risk Champions will assess the risk by determining its probability of occurrence and its impact with an objective of reporting key risks to the CRO.

Key responsibilities of the Risk Owners include:

- Communication of evolving new risks and changes in the status of previously identified risks
- Reporting failures of existing control measures
- Updating the risk registers of their domains
- Educating Risk Champions with Risk Management activities
- Providing ERM with controls and "good to have" controls for critical process of their domains

Risk Owners will ideally be process heads and/or functional heads

6.1.7 Risk Champions

Risk Champions will assist Risk Owners in implementing and monitoring risk mitigation plans. Risk Champions will be designated by the Risk Owners. Risk Champions will ideally be process owners of a executives under Risk Owners.

6.2 Risk Management Activity Calendar

Activity	Frequency
Risk Register Review report to be submitted by risk owners to the CRO	Biannually
Review by Risk Management Committee	Biannually (with gap between two meetings no more than 180 days)
Risk Management Committee Meeting	Biannually (with gap between two meetings not more than 180 days)
Review of Top Risks by Board	Annually

6.3 Aligning Internal Audit with Enterprise Risk Management

It is important for an organisation to align risk management and internal audit functions. The output of risk management activities will be incorporated into the development of the annual internal audit plan. Similarly, critical risks identified through internal audit will be evaluated for inclusion in the Enterprise Risk Register. The evaluation will be carried out by the CRO along with the Executive Risk Management Council and finally reviewed by the RMC.

7. APPROVAL OF THE POLICY

The Risk Management Committee will recommend to the Board. The Board will approve the Risk Management Policy.

8. REVIEW OF THE POLICY

This policy will be reviewed and revised:

- If there is a change in regulation/requirements by regulatory body
- Once in two years

Document Control

All changes to the process document can be made only by the Document Owner.

Document Owner	Board of Directors of GMM Pfaudler Ltd.
Current Version:	3.0
Issue Date:	February 12, 2015

Revision History		
Version	Revision Date	Revision Description
1	October 25, 2018	1 st Amendment
2	September 20, 2021	2 nd Amendment
3	January 16, 2023	3 rd Amendment