POPULAR VEHICLES AND SERVICES LIMITED
RISK MANAGEMENT POLICY

Name of document	RISK MANAGEMENT POLICY
Version	2.0
State whether Policy/Code/Manual/Guideline	Policy
Issuing Authority	Risk Management Committee
Effective date of Version 1.0	10th June 2021
Release date of current version	11th February 2025
Last amended on	--
Version history	1) 1.0 initial version dated 10th June 2021 2) 1.1 version dated 14th August 2023 3) 2.0 version dated 11th February 2025

POPULAR VEHICLES AND SERVICES LIMITED

RISK MANAGEMENT POLICY

1. INTRODUCTION

Popular Vehicles and Services Ltd (“PVSL” or “the Company”) with its subsidiaries form a diversified automobile dealership in India for renowned OEMs with a diversified and fully integrated business model catering to the complete lifecycle of vehicle ownership, right from sale of new vehicles, servicing and repairing vehicles, distributing spares and accessories, to facilitate sale and exchange of pre-owned vehicles, operating driving schools and facilitating the sale of third party finance and insurance products. Headquartered in Kochi, Kerala, PVSL is the flagship company of the renowned Kuttukaran family, a name which is familiar to the automobile industry for more than eight decades.

This (revised) Policy, after suitably considering the applicable Indian Regulations[Note1] , the industry and organisational context, aims at formalizing a process to deal with risks by building on existing management practices, knowledge and structures, and outlines its risk management framework.

2. SCOPE AND AUTHORITY OF THE POLICY

This Policy replaces the current policy effective 11th February 2025.
This Policy shall be under the oversight and advisement of the Risk Management Committee of the Board of Directors (“the Board”). The Board is responsible for approving any changes to this Policy. This Policy may be reviewed at least once in every two years.

3. RESPONSIBILITY FOR RISK MANAGEMENT

Risk management is part of Company management’s responsibility, and they should take accountability for identification, appropriateness of mitigation, as well as implementing, tracking, and reporting of risks in line with this Policy.

A Risk Leadership Council (represented by members from management) is responsible for the Company’s risk management program.

4. SCOPE OF RISK MANAGEMENT

As a renowned player in the auto retail segment, the Company is potentially exposed to a multitude of internal and external risks. The Company’s risk management program is designed to actively address key enterprise-wide risks relevant in the medium-term (i.e., up to twenty-four months). Additionally risks beyond the horizon may be identified and placed on watchlist.

5. RISK MANAGEMENT OBJECTIVES

The Company’s risk management program is designed to achieve the following objectives:

- Better understand the Company’s risk profile.
- Improve compliance with good corporate governance guidelines and practices, as well as laws and regulations.
- Identify key risks and potential crises scenarios that can impact business objectives.
- Proactively manage risks and drive timely mitigation.
- Optimize costs and effort needed to manage risks.
- Build necessary resilience via crises management or business continuity plans.

6. DEFINITIONS

Risk: The possibility that events will occur and affect the achievement of business objectives.

Risk Management: The culture, capabilities, and practices, integrated with performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

Risk Appetite: The maximum amount of risk an entity is willing to absorb in the pursuit of its business objectives. This may be applied both qualitatively and quantitatively.

7. RISK MANAGEMENT PROCESS [Note 2]

Risk criteria, risk identification, risk assessment, risk response, monitoring, review and reporting processes may be applied at all levels - strategic, operational or project.

Communication and consultation with appropriate external and internal stakeholders may take place within and throughout all steps of the risk management process.

Setting a Risk prioritisation framework

The Company shall have a documented risk prioritisation framework consistent with the organisation context and scope. The framework shall consider the nature and type of risks, the likelihood, the impact (or consequence) and velocity of risks.

While risk criteria are established at the beginning of the risk assessment process, they should be periodically reviewed and amended, when necessary.

[Annexure 1 contains the current version of the Company’s Risk Prioritisation Framework, together with the Risk Appetite]

Identifying and assessing risks:

Risk Identification:

The Company shall identify new or emerging risks, as well as changes to existing risks that may directly or indirectly impact the achievement of its business objectives.

As an when a new risk is identified, it shall be updated in the risk register. Techniques for risk identification are listed in Note 3. The register of risks and concerns shall be periodically reviewed and updated.

The Company may organize the risk register by categories so that similar risks are grouped together and provide a portfolio view across the enterprise. The Company may choose to additionally re-group risks as required by regulation.

Assessing risks:

Company management determines the relative severity of risks to select an appropriate risk response, allocate resources, and support management decision-making and performance.

Risk assessment shall be carried out by applying the risk prioritization framework. Due care needs to be taken to assess the frequency/probability and impact, and relevance of risks. Wherever possible, objective or quantitative data such as metrics and historical losses may be considered.

A portfolio view of relevant risks may be developed and focusing on the key risks helps boards and management focus greater attention on the achievement of strategy. A detailed taxonomy may be developed and applied covering the following key risk areas for the Company:

1. Financial Risks
2. Commercial and Operational Risks
3. Sectoral Risks
4. Sustainability and ESG risks
5. Information and Cyber Security
6. Crisis, Interruption and BCP

The outcome of risk assessment should be recorded, communicated, and confirmed by management.

[Annexure 2 contains the taxonomy and hierarchy of risks and an indicative version of the Company's Enterprise Risk Heatmap]

Responding to risks

For all risks identified, management selects and deploys one or more risk responses. In doing so, management may consider the following factors as key considerations: business context, costs and benefits, obligations and expectations, prioritization of risk and risk appetite.

Risk responses may fall within the following categories:

- Avoid: Action is taken to remove the risk. Choosing avoidance suggests that the organization was not able to identify a response that would reduce the risk to an acceptable level of severity.
- Transfer: Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk.
- Reduce: Action is taken to reduce the severity of the risk.
- Accept: No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite.
- Pursue: Action is taken that accepts increased risk to achieve improved performance.

Additionally, management may identify contingency plans for high severity and high velocity risks to minimize the impact of significant risk events. The company's risk prioritisation framework referred above, also determines the priority and urgency of the risk responses.

[Annexure 3 contains the current version of the Company's Risk Register template that provides the assessment and response to identified risks]

Risk reporting

The risk management process and its implementation should be documented and reported, with due consideration applied to their use, information sensitivity, internal and external context.

Risk reporting may include any or all the following:

- Portfolio view of risk(s)
- Analysis of root causes
- Sensitivity analysis
- Analysis of new, emerging, and changing risks
- Key performance indicators and measures
- Trend analysis
- Disclosure of incidents, breaches, and losses
- Tracking enterprise risk management plans and initiatives

Monitoring and Review:

Management shall develop suitable oversight structure, governance and reporting mechanisms with regards to risk management. Additionally, suitable Responsibility, Accountability, Consult or/and Inform (RACI) matrix may be developed to clarify the roles, responsibilities and accountabilities of various stakeholders.

Relevant management members may form a Risk Leadership Council to periodically review progress of risks, guide the risk management program and help in evaluating and approving decisions and initiatives involving risk.

The Risk Management Committee of the Board should engage with the management on the Company's key risks twice in a year, whereas the Company's management may review the risks more frequently and granularly, e.g., once every quarter. The Chief Risk Officer acts as the secretary to the Risk Management Committee

[Annexure 4 contains the current version of the Company's risk management Oversight and Governance structure and the roles and responsibilities]

8. MAKING IMPROVEMENTS

The Company may continually improve suitability, adequacy, and effectiveness of the risk management program.

In addition to committing to provide necessary resources, there should be a periodic review and improvement of the risk management policy and framework in response to an event or change in circumstances.

Notes

<u>Note 1</u>

Sec 134 of the Companies Act 2013 - requires directors to confirm the Company's Risk management policy and framework.

SEBI (**LODR, May 2021**) requires Top 1000 Companies by market capitalization a mandatory set-up of Risk Management Committee (RMC) and to specifically cover risk areas including ESG & BCP. Accordingly, it is proposed that the role of the RMC shall inter alia- include the following:

1) To formulate a detailed risk management policy which shall include:

- *A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee*
- *Measures for risk mitigation including systems and processes for internal control of identified risks*
- *Business continuity plan*

2) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;

3) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;

4) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;

5) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;

6) The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.

Note 2

The Company proposes to adopt a simple and scalable risk management program that eventually aligns to the best practices put forward by frameworks such as COSO ERM 2017.

Note 3

Depending on the degree of uncertainty, several Risk Identification techniques are possible to be used, ranging from low complexity and low on resources to high on complexity and resources and capability. A few of them are indicated below:

- Industry analysis, external reports
- Data tracking: Tracking past events that help predict future occurrences.
- Interviews and Workshops
- Key performance indicators and other risk metrics
- Process analysis or other techniques that are prevalent in their manufacturing, quality, safety, or business continuity processes such as FMEA, HAZOP or Business Impact Analysis

Annexure 1: The Company's risk prioritisation framework

Impact (*Synonymous with Severity*)

Impact Attributes	Measurement	1. Minor	2. Low	3. Moderate	4. High	5. Critical
Regulatory	Loss of Credibility with regulators	Potential to receive notice or actual receipt of complaint with no penalties.	Potential to receive notices / actual receipt of complaint with < Rs. 10k in potential penalties	Potential to receive notices / actual receipt of complaint with > Rs. 10k but less than < Rs. 1 lac in penalties	Potential to receive notices / actual receipt of complaint with > Rs. 1 lac but less than Rs. 10 lacs in potential penalties	Suspension of license to operate or closure of operations OR/AND Potential penalties in excess of Rs. 10 Lacs OR/ AND Prosecution of employees of the Company.
People and Environment	Accident severity rate, injury, loss of life and/or harm to environment	Near misses or potential injuries to people	First-aid type of injuries to people	Reversible occupational illness OR injuries affecting few people but are able to return to work within a few days	Injured persons unable to return to work within a few days OR minor or major issues impacting surrounding communities, reversible in the short term.	Fatal injury OR Multiple 'High' injuries OR Irreversible occupational illness which reduces life expectancy OR Irregularities having potential for long-term or irreversible damage in surrounding communities,
Reputation/Public Profile	Negative impact on Customer and Investor confidence	Minor customer annoyance	Customer dissatisfaction OR Investor/Analyst enquiries	Customer dissatisfaction impacting payments or future ordered quantities OR Impact to stock prices of <2%	> 20% customers dissatisfied impacting payments or future ordered quantities OR Impact to stock prices of <10%	Potential to lose key customer (s) OR Impact to stock prices of >10%
Financial	Impact to PBT	< Rs. 10 Lacs	Rs. 10 Lacs - Rs. 50 Lacs	Rs. 50 Lacs - Rs. 2.5 Cr	Rs. 2.5 Cr - Rs. 10 Cr	> Rs. 10 Cr

Frequency and/or Likelihood:

Aspect	Measured as	1.Rare	2.Unlikely	3.Possible	4.Likely	5.Expected
Probability of risk	%	Up to 1%	1 to 5%	5 to 20%	20-50%	=>50%
Frequency	Frequency	May exceptionally occur	May occur up to once in 20 years	May occur once in up to 5 years	May Occur once in up to a year	May occur more than once a year

Annexure 2 : Risk Taxonomy

S No	Risk Category	Definitions
Financial risks		
1	Treasury Risks	External financial risks exposures from interest rates, foreign exchange and/or commodity prices. May be further categorised into Credit, Currency, Interest rate or Commodity risks.
2	Financial Reporting	Inaccurate recording and reporting of all financial transactions in the proper accounting period in accordance with existing standards. It includes significant or material weaknesses resulting from inadequate financial or internal controls. It also includes taxation risks or failure to minimize tax obligations. May be further categorized into Internal Control failure (IFC) , Misstatements and Errors and Taxation risks, Investor Relations
3	M&A and Restructuring	Failure to effectively execute and integrate a strategic acquisition, merger or divesture intended to achieve business or acquisition objectives. May be further categorized into Potential impairment, Synergy loss, Failure to integrate or Successor liabilities
4	Investment risks	Failure to meet the requirements of a portfolio of capital investments and obligations based on specified commitments or planned capital allocation.
5	Liquidity and Cash Flow	Failure to administer, monitor and manage cash related activities to ensure liquidity. May be further categorized into Liquidity and Cost/Efficiency management
6	Credit risk	Potential financial loss that a dealership or lender may face if a customer fails to meet their loan or lease payment obligations. It includes products and services provided by the Company on credit
Auto retail Sectoral risks		
7	Inventory Holding and Supply chain risks	Potential financial losses that dealerships may incur due to unsold vehicles. These include other supply chain risks such as delays in vehicle delivery, disruptions in parts supply, and fluctuations in transportation costs
8	Demographics & Economic risks	Unfavourable changes in the population's characteristics, such as age, income levels, and consumer preferences. Includes risk impacts resulting from changes in the broader economy, such as fluctuations in interest rates, inflation, and unemployment rates. These risks can affect consumer purchasing power, vehicle demand,
9	Disruptive Platforms and Technologies	Emergence of new technologies or digital platforms that change consumer behavior, market dynamics, or competitive landscapes. These risks can affect traditional business models, sales channels . Some examples are online insurance portals focused on auto industry, emergence of EVs etc

S No	Risk Category	Definitions
10	Evolving Business Models	Shifts in how vehicles are sold and serviced, such as the rise of subscription services, online sales platforms, and shared mobility solutions. These changes can affect traditional dealership operations, revenue streams, and customer relationships.
Commercial and Operational Risks		
11	Business/Growth risks	Inability to grow or failure to fund growth initiatives and meet stakeholder expectations in the management & execution of projects, execute strategies and meet goals and objectives. Risks may further be categorized into Project execution, Failure to innovate, or expansion
12	Customer and Competition risk	Actions of competitors or entrants to the market that impacts our competitive position and includes changes in customer preferences and other demand dynamics. Risks may be further categorised into Customer preferences, Competitor actions, Pricing.
13	HR/People risks	Risks associated with culture, organizational structure, communication, recruitment, performance management, remuneration, learning & development, retention, and industrial relations, including supporting systems, processes and procedures. Risks may be further categorized into Talent attraction/retention, Succession & Keyman risks, Succession , Skill-shortage / Competency , Compensation & Benefits
14	Safety and Health	Risks relating to safety of customers and employees' health and security at Company locations. It also covers employee and customer safety from health and safety events /incidents while using company assets. Risks may be further categorized into Accidents, Fire, Security Lapses, Contractor safety, Terrorist attacks or Bombings
15	Regulatory risks	Risk relating to non-compliance with legislations including labour laws, fiscal laws, adequacy of financial reporting & disclosures, regulations, internal policies and procedures. Risks may be further categorised into Regulatory change, Data privacy and Compliance excursions
16	Geopolitical risks	The occurrence of political actions in a country where the organization has invested human and capital resources and/or where the impact can threaten the organization's future cash flows and profit targets. Risks may be further categorized into Government preferences, War or Civil unrest

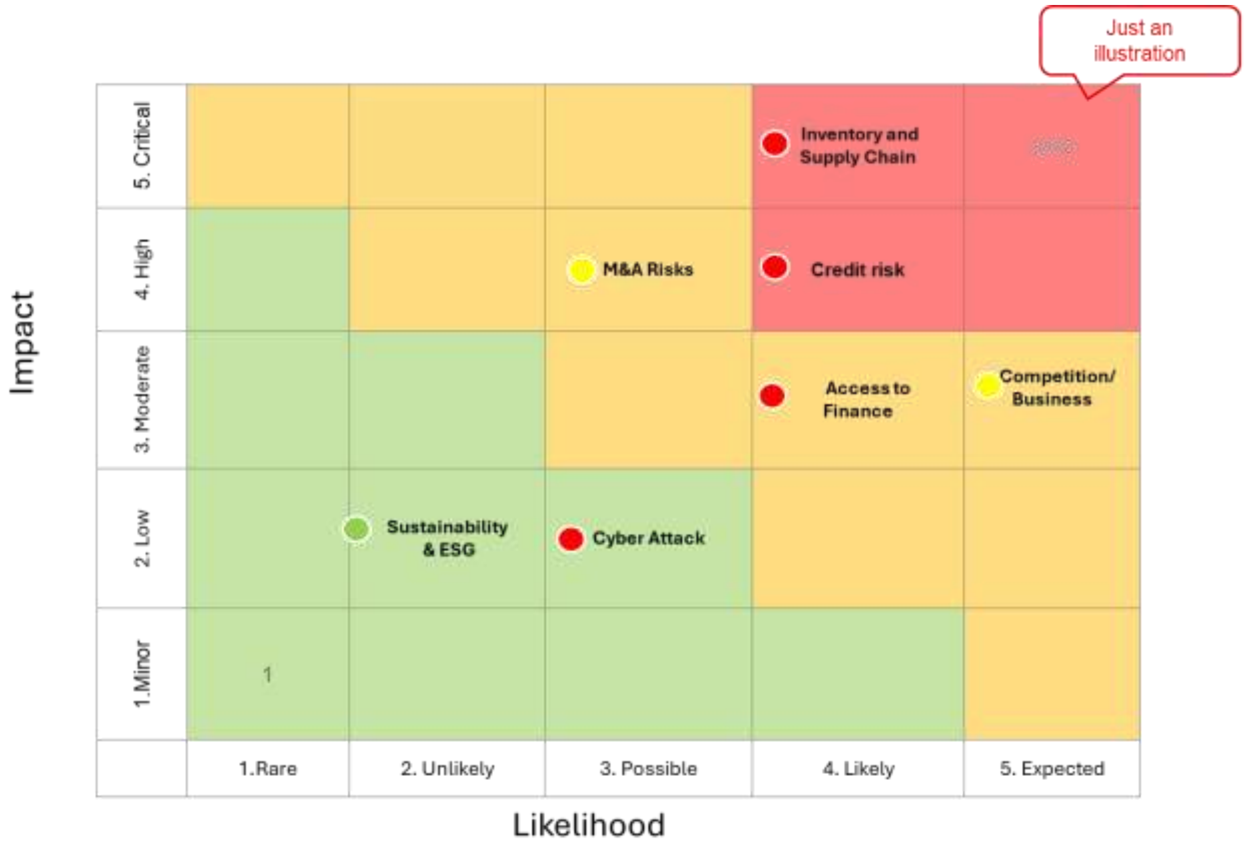
S No	Risk Category	Definitions
17	JV/Alliancing risks	Unproductive, high-risk or otherwise not closely managed alliance partnerships that can lead to lost time and investment, product and/or service failures.
18	Business Model risks	Risks and uncertainties associated with the company's business. It includes inflexible cost structures, seasonality, dependence on external variables as well as excessive leverages. Risks may be further categorized into Seasonality, Inflexible cost base
19	Legal risks	Inability of the organization to comply with important transactions, enforce contractual agreements and includes inherent risks and liabilities assumed in legal contracts. It also includes exposure from active litigation. Risks may be further categorised into Contract commitments, Unlimited liabilities, etc.
20	Ethics and Fraud	The absence of formal standards of employee code of conduct that are intended to direct and influence the way business is conducted, above and beyond the letter of the law as well as potential unethical acts committed by Company employees or other stakeholders that may negatively impact the company May be further categorized as Claims and Billing, Management over-ride, Collusions/Conflict of Interest, Fraudulent reporting
21	Concentrations	Key dependencies on location, customer, supplier or specialisation may lead to potential risk exposures in case of any risk event. These could further be categorised as Location, Customer, Supplier and Specialisation
Sustainability and ESG risks		
22	Environmental risks	Risks associated with environment pollution including emissions, water and disposal of hazardous and non-hazardous waste and plastics. Risks could be further categorized into hazardous waste disposal, Emissions, Plastic waste, Environmental non-compliances
23	Climate Change risks	Inability to plan for or recover from extreme seasonal weather fluctuations that impact operations and financials. It includes failure to prepare for climate change transitions in line with national or international deadlines. Risk may be further classified into Physical risks and Transition risks
24	Stakeholder expectations	Ability to maintain stakeholder confidence in meeting goals and objectives in relation to ESG expectations and other material topics. Risks may be further categorized as ESG ratings, Social audits, ESG investments and Greenwashing risks
Information and Cybersecurity		
25	Information security risks	Failure to protect internal and external access to the data they provide from theft, viruses, sabotage or improper use. In includes non-availability of timely information as well as incorrect information that may negatively impact decision making. It also includes improper access to or abuse of Unpublished Price Sensitive Information (UPSI). Risks could be further categorized as Confidentiality (including UPSI), Data Privacy, Information availability and Data Integrity

S No	Risk Category	Definitions
26	Cybersecurity risks	Exposure or loss resulting from a cyber-attack or data breach and includes ransomware events, and failure to comply with regulatory protocols in relation to Cybersecurity protocols in a timely manner. (eg NIST, time of reporting etc). Also, the IT/Cyber components of DPDP regulation will need to be covered. It can be further categorized into Ransomware, Data security , Data Privacy (DPDP)
Crisis, Interruption and BCP		
27	Brand/Reputational risks	Risks associated with appropriateness/adequacy of external communication & PR and indirectly with customer sources, competition, brand management & brand licensing and reputation of the company. These may be further classified as External communications, Corporate branding and Social media risks.
28	Inadequate Crisis management	Business continuance and resource conservation risk associated with during Calamities and disasters. Includes the risk of diseases and pandemics to adversely impact patients, workforce and supply chain. It also includes, risks associated with infection control. Can be further classified into Preparedness for Flood/Storms, Fire events, Earthquake, Endemic/Pandemics
29	Inadequate Business Continuity Planning	Failure to undertake the appropriate advance planning related to critical processes to ensure the ability to recover and maintain business operations in the event of a disruption due to internal, third party, physical or natural circumstances. Includes further classification of Power outage, Utilities interruption, Supply shortage, Critical staff and IT/DR

The above list may be modified in future to add/modify new risk categories or sub-categories that may emerge. Any interim additions to this list may be incorporated with approval from the Risk Office. Additionally, a Level 2 taxonomy may be developed for each of the above L1 risk categories.

The Company's Indicative Heat-Map representation

(e.g., Top 10 risks)



Risk rating	Response
High	Immediately reduce + Continency plan for High velocity risks
Moderate	Reduce based on cost: benefit
Low	Accept/Improve

Within the group **Risk Velocity** can be used to prioritize responses or actions

- Instant - Impact is Immediate or <1 month
- Evolving - Impact in 1 to 6 months
- Gradual - Impact in > 6 months

*Likelihood and Impact Scales will be defined. Prioritisation will be developed

Annexure 3: The Company's risk register format

1. Risk ID No.	2. Risk Category	3. Risk Statement (Event, Cause and Consequence)	4.Additional details

5. Likelihood/Frequency Score	6. Impact Score	7. Overall Score	8. Risk Owner

9. Risk response (Mitigation, Control or response) or Contingency	10. Cost of response	11. Mitigation owner(s) or Risk Action owner(s)	12. Lead Metrics

13. Lag metrics	14. Linkage to Scorecard/ Business Objective	15. Current risk triggers/exposures or recent events	16. Business/Function Segment, Location and Geography

Additional fields may be considered for analytical purposes such as Cost of mitigation. Procedure(s) for updating the risk register may be separately prepared on a need-basis.

Annexure 4a : The Company's Risk Oversight Structure and Governance and RACI framework:

CEO : Chief Executive Officer,
CHRO : Chief Human Resource Officer ; CFO = Chief Financial Officer
CRO: Chief Risk Officer; PCH : Profit Centre heads

RACI framework		Role titles
R	**Responsible**: The individual(s) who complete the task. The individual(s) responsible for dealing with the risk mitigation action or decision. Responsibility can be shared.	Mitigation Owner or Risk Action owner
A	**Accountable:** The individual who is ultimately answerable for the activity or decision. This includes "yes" or "no" authority and veto power. Accountability should not be shared.	Risk Owner
C	**Consulted:** Is the individual (typically subject matter expert) who may be consulted prior to a final decision or action.	SME / Domain expert
I	**Informed:** This is individual (s) who needs to be informed and updated on risks or after a decision or action is taken.	Management, Board, etc

Annexure 4b : Roles and Responsibilities

Risk Management Committee (Board)

Responsibilities

- Formulate, review or approve the company's risk management policy.
- Conduct policy reviews at least once every two years, considering industry dynamics.
- Define suitability of enterprise risk management by engaging with management.
- Independently enable oversight of management of risks.
- Monitor risk management policy implementation, evaluating adequacy of risk systems.
- Promote Risk Awareness in line with entity maturity

Governance Cycle	Half-yearly

•Understand risk sources, appetite, and portfolio view; assess significant risks and responses provided by Management and the Risk office.

• To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;

Risk Leadership Council (Management)

Responsibilities

- A management level committee consist of CxOs and others as may be required for ensuring effective risk management process and guiding the risk office
- Assuming overall responsibility for effective enterprise risk management, including the processes used to identify, assess, prioritize, respond to, and report on risk.
- Considering and discussing emerging risks.
- Defining roles, responsibilities, and accountabilities at different levels of management.
- Reviewing the entity's risk profile.
- Reviewing acceptable variation in performance and taking action where appropriate.
- Develop risk appetite statements together with the Domain/Function owners for core risk areas

Governance Cycle	Quarterly

• Formulate and approve the risk management policy
• Communicating the status and progress of enterprise risk management process to the Board (as required).

Risk Office (CRO)

Responsibilities

- Assisting the Risk management committee in fulfilling their respective risk oversight responsibilities.
- Establishing ongoing enterprise risk management practices suitable for the entity's needs.
- Provide necessary guidance and support to functional and business risk teams in carrying out risk identification and reporting activities.
- Periodical review with Management Council on emerging risks and mitigation status
- Review metrics and risk exposures on a periodic basis with the risk owners
- Facilitating Risk workshops
- Monitor the progress of mitigation

Governance Cycle	Quarterly

- Communicate with Risk Management Leadership Council, about the status of enterprise risk management, which includes discussing severe risks and emerging risks.
- Communicate with Risk Management Committee and reporting of Risk MIS in RMC meetings – Half yearly

-----End of document---