Aurionpro Solutions Limited

Enterprise Risk Management Framework and Policy

Confidential

Revision History

Version	Date	Prepared By	Reviewed By	Approved By	Changes / Remarks
1.0	08.10.2024	Risk Team		Board of Directors	New Document – Discussion Draft

Contents

1. Introduction 4

2. About Aurionpro Solutions Limited 4

3. Foundation of the ERM Policy Framework 4

4. Risk Strategy and Appetite 4

5. ERM Alignment with Planning, Strategy & IFC: 5

6. Risk Management Objectives 5

7. Risk Management Approach 5

- *Key Risks for the Organization: 5*
- *Risk Assessment and Evaluation 7*
- *Risk Response and Treatment Schedule 7*
- *Risk Monitoring and Review 8*
- *Continuous Improvement (CI): 8*

8. Office of Enterprise Risk Management 8

9. Enterprise Risk Management Framework at Aurionpro Solutions 9

10. Key Roles and Responsibilities 9

11. Review and approval of the policy 10

12. Limitations and Amendment 10

1. Introduction

The **Enterprise Risk Management (ERM) Framework** at Aurionpro Solutions Limited provides a comprehensive and structured approach to identifying, assessing, managing, and monitoring risks that may impact the company's objectives. This policy aligns with Section 134 of the **Companies Act**, 2013, **SEBI** (Listing Obligations and Disclosure Requirements) Regulations 2015, and the **COSO** Framework.

2. About Aurionpro Solutions Limited

Aurionpro Solutions Limited is a global technology company that help enterprises accelerate Digital Innovation securely and efficiently. It has specialisation in providing innovative software solutions and services across various sectors, including banking, financial services, and Government sector. Aurionpro has established itself as a leader in digital transformation, delivering cutting-edge products that enhance operational efficiency and customer experience.

Vision, Mission, Business Strategy and Strategic Objectives of the company are as follows:

- **Vision:**
  - To be a global leader in providing Advance and Accelerated Platform-led Transformation, guiding businesses to ADAPT to a new paradigm in the digital world.
- **Mission:**
  - To deliver cutting-edge solutions in banking, mobility, payments, and government sectors that enhance operational efficiency, foster digital transformation, and ensure seamless user experiences while maintaining the highest standards of security and compliance.
- Risk Management Philosophy:
  - To proactively identifying, assessing, and mitigating risks to ensure resilience, innovation, and secure digital transformation arising from strategy and business objectives.

3. Foundation of the ERM Policy Framework

The ERM policy is supported by a comprehensive suite of administrative tools, policies, directives, and Standard Operating Procedures (SOPs), providing a roadmap for effective risk management across all organizational levels.

4. Risk Strategy and Appetite

Aurionpro has carved out a Strategic roadmap for achieving long term and short-term goals that include growth of revenue segments, nurturing talent, operational excellence and client delight. Board and Executive team set objectives, analyzes competitive environments, and allocates resources to maximize success across identified goals.

Board has prepared a risk strategy plan that outlines how the organization intends to manage risks to achieve its core objectives. It involves identifying potential risks, assessing their impact, and developing strategies to mitigate them. The key components of the risk strategy include: -

1. **Risk Appetite**: This defines the level of risk the company is willing to accept to achieve its goals.
2. **Risk Tolerance**: This refers to the acceptable variation in outcomes related to specific risks.
3. **Risk Capacity**: This is the maximum amount of risk the company can handle without jeopardizing its objectives.

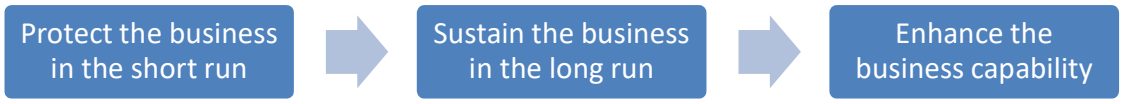
5. ERM Alignment with Planning, Strategy & IFC:

- **Integration with Business Strategy:** ERM is aligned with the company's business strategy, planning, decision-making, and Internal Financial Controls (IFC).
- **Inherent in Strategic Planning & Adapting Business Models to Mitigate Risks:** Risk management is integral to strategic planning, ensuring alignment between risk appetite and strategy.

6. Risk Management Objectives

Aurionpro's ERM aims to proactively identify, assess, and mitigate risks to ensure operational resilience, regulatory compliance, and sustainable growth. The primary objective is to manage risk exposures within the company's risk appetite, minimizing unexpected financial losses and deviations from anticipated outcomes.

Risk Management Objectives



Risk Management Approach

Risks at Aurionpro Solutions Limited may arise from internal and external factors, including unpredictable events. These risks can impact assets and affect organizational strategies, operational and financial objectives, earning capacity, and financial position etc.

Aurionpro's risk management process is designed to proactively address these risks through the following key steps:



- **Key Risks for the Organization:**

Sr No	Key Risk	Risk Definition
1.	Strategy Risks	Risks arising from inadequate or ineffective business strategies, poor strategic decision-making, or misalignment between the company's strategy and market realities. These may result in the loss of competitive edge or failure to achieve long-term objectives.
2.	Financial and Investment risks.	Risks related to the company's financial health, including cash flow management, liquidity issues, capital allocation, or inadequate returns on investments. They also encompass exposure to currency fluctuations and interest rate changes.
3.	Market risks	Risks posed by external market forces such as economic downturns, changes in customer demand, competitive pressures, or geopolitical factors, which could affect the company's market position or growth potential.
4.	Customer risks and client concentration risks	Risks associated with over-reliance on a limited number of key customers or sectors, which may lead to revenue volatility if customer needs change or contracts are lost. Failure to meet customer expectations can also damage relationships and revenue.
5.	Peer risks	Risks of falling behind competitors in terms of innovation, product offerings, or market share. This includes the risk of not anticipating competitor actions or market changes that could erode Aurionpro's market position.
6.	Cyber Security risks	Risks related to data breaches, cyberattacks, or system vulnerabilities that could compromise sensitive information, disrupt operations, or result in financial losses and reputational damage. This also includes data privacy risk, source code risk and open-source software risk.
7.	People risk	Risks related to recruitment, retention, and development of talent. This includes the risk of losing key personnel or failing to maintain a productive and engaged workforce, which could impact operational efficiency and innovation capacity.
8.	Reputational risks	Risks of damage to the company's reputation due to negative public perception, operational failures, unethical practices, or external events, which could lead to loss of customer trust, market share, and stakeholder confidence.
9.	New Country risks	This risk includes political instability, regulatory differences, cultural and language barriers, currency fluctuations, and unfamiliar legal environments, which could negatively impact the company's ability to operate effectively in the new region.
10.	Legal and compliance risks	Risks related to non-compliance with legal, regulatory, or contractual obligations, including changes in laws and regulations. Non-compliance can lead to fines, legal disputes, or sanctions that could negatively affect the company's operations.
11.	Product Implementation risks	This risk encompasses factors such as delays, technical issues, inadequate resource allocation, misalignment with client needs, or failures in meeting performance expectations affecting adversely to project timelines, customer satisfaction or leading to contract breaches if not managed effectively.
12.	Cloud Infrastructure risk	This risk refers to the potential vulnerabilities and uncertainties associated with using cloud-based services and infrastructure. It includes data breaches, service disruptions, vendor lock-in, and the potential for unauthorized access to sensitive information due to cloud provider failures or misconfigurations.

Sr No	Key Risk	Risk Definition
13.	Business Continuity Risks	This is the risk of unplanned interruptions in the business on account of an accident, disaster, emergency or threat.
14.	Intellectual Property Infringement risk	This risk refers to the potential for unauthorized use, violation, or misappropriation of intellectual property (IP), such as patents, trademarks, copyrights, or trade secrets. This risk can arise from third parties infringing on the company's IP or from the company inadvertently infringing on the IP rights of others.
15.	ESG / Climate Risk	Climate risk includes the adverse impacts associated with environmental, social, and governance (ESG) factors, especially climate change. These risks cover regulatory changes, environmental hazards, resource scarcity, and shifting market expectations related to sustainability and corporate responsibility.

Above is an illustrative list and not an exhaustive one.

- ## Risk Assessment and Evaluation

Once risks are identified, they are evaluated on a two-dimensional matrix using a qualitative rating of the likelihood of the event occurring and the scale of the possible consequences. This analysis involves combining the consequences and likelihood to produce a risk level, determining which risks need treatment and which can be accepted. Key tools include:

1) Periodic Risk Control Self-Assessment (RCSA) evaluation
2) Assessing strategic changes in business operations
3) Evaluating key industry changes
4) Monitoring regulatory changes
5) Conducting loss data analysis
6) Investigating internal/external frauds
7) Analysing profitability

- ## Risk Response and Treatment Schedule

Once risks are identified a risk response strategy will be defined which will include:

Tolerate (Accept)	Treat (Mitigate)	Transfer	Terminate (Avoid)
•**Actions:** Acknowledge the risk and decide to accept it without taking further action. This approach is suitable when the cost of mitigation is higher than the potential impact of the risk. •**Examples:** Documenting the rationale for acceptance, monitoring the risk, and preparing contingency plans	•**Actions:** Implement measures to reduce the likelihood or impact of the risk. This involves taking proactive steps to lessen the risk's potential effects. •**Examples:** Improving processes, enhancing training, upgrading systems, or adding controls	•**Actions:** Shift the risk to a third party. This approach is often used when the risk can be better managed by an external entity. •**Examples:** Purchasing insurance, outsourcing certain functions, or entering into partnership	•**Actions:** Take steps to eliminate the risk entirely. This strategy is used when the risk poses a significant threat and can be completely removed. •**Examples:** Changing strategies, discontinuing certain activities, or altering project scopes

- ### Risk Monitoring and Review

The Company regularly monitors and reports risks and mitigation plans to senior management and Board Committees. This allows a clear understanding of overall risk exposure and equips leaders to take appropriate measures. The risk monitoring framework includes:

- Key Risk Indicators
- RCSA testing results
- Solvency position and stress testing results
- Vendor/Partnership performance evaluation results
- BCP testing results
- Loss event data analysis

- ### Continuous Improvement (CI):

All risk management processes are regularly reviewed, incorporating lessons learned from previous incidents to enhance future responses.

7. Office of Enterprise Risk Management

The Company may establish an Office of Risk Management (Risk Office) with sufficient independence and authority for ERM, headed by the 'Chief Risk Officer' (CRO). The objectives of the unit include:

- Embedding a consistent approach to risk-based decision making in company processes and culture, aligned with strategic objectives.
- Minimizing the adverse impact of risks on the enterprise and its operations, thus enhancing long-term competitive advantage.
- Identifying opportunities to convert risks into opportunities for improved performance.
- Designing and implementing an ERM Framework, monitoring key risks and mitigation plans, and reporting these to the CEO, CFO, CS, Group Compliance Officer and other necessary management personnel and the Risk Management Committee (RMC) of the Board.

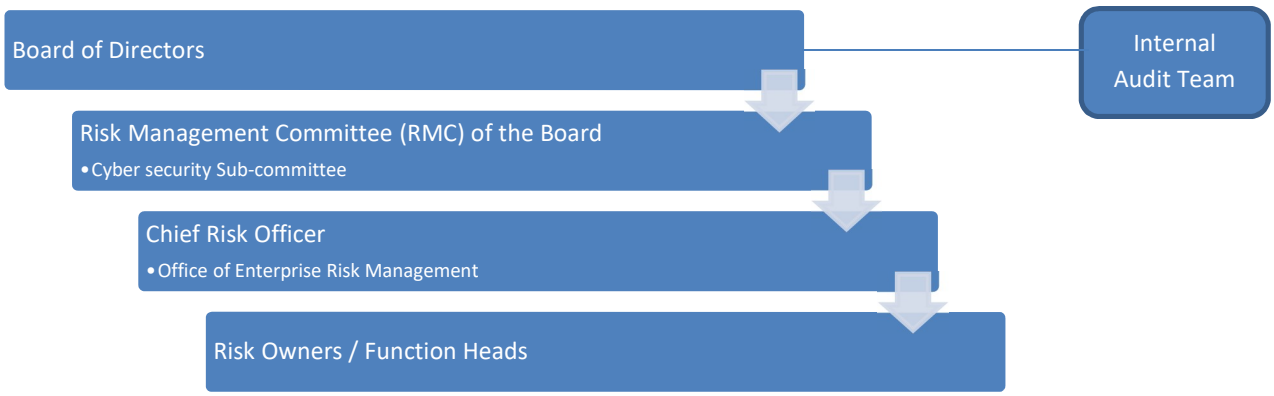
The unit will collaborate closely with related risk management functions such as legal, compliance, secretarial, information security, finance, and data privacy.

8. Enterprise Risk Management Framework at Aurionpro Solutions

The ERM Framework, based on industry standards, addresses all internal and external risks, including strategic, operational, legal, and compliance risks etc. It prescribes procedures and guidelines for:

- Contextualizing risks linked to strategic objectives
- Identification, assessment, and mitigation of risks
- Internal controls, communication, monitoring, and governance
- Utilizing risk indicators for proactive identification

Risk management enables effective resource allocation based on Risk Impact Ranking and Risk Appetite, supporting strategic decision-making. The Board of Directors hold primary responsibility for risk management, supported by the entire organization. The Enterprise Risk Management structure at Aurionpro Solutions is as follows:



9. Key Roles and Responsibilities

- **Board of Directors:**

The Board is responsible for framing, implementing, and monitoring the risk management plan for the Company. Upon the Risk Management Committee's recommendation, the Board will adopt the Risk Management Policy and critically review the risk governance and monitoring mechanisms. The Board shall meet at least once a year to review the top risks faced by the Company and the status of their mitigation plans.

- **Audit Committee:**

The Audit Committee will meet at least once a year to oversee the risk management and internal control arrangements. It will also evaluate the Company's internal financial controls and risk management systems.

- **Risk Management Committee (RMC):**

The Risk Management Committee (RMC) assists the Board by establishing policies, guiding their implementation, and monitoring their effectiveness. It serves as a platform to discuss and manage significant business risks, periodically assessing these risks and reviewing important indicators. The RMC will formulate and monitor the implementation of the Risk Management Policy.

- **Chief Risk Officer (CRO):**

The CRO leads the design and implementation of the company's ERM strategy, aligning it with corporate objectives and regulatory requirements. This role includes developing risk mitigation plans and ensuring timely reporting of key risks to the Board of Directors and senior leadership. The CRO monitors the effectiveness of risk responses and ensures compliance with risk policies.

10. Review and approval of the policy

The Chief Risk Officer shall propose this Policy or any changes to the RMC of the Board. This Policy shall become effective upon their approval and will be reviewed as deemed necessary by the RMC, at least once every two years, considering changing industry dynamics and evolving complexity

11. Limitations and Amendment

In the event of any conflict between the provisions of this Policy and the Companies Act, 2013, and relevant regulations of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("Applicable Law"), the provisions of Applicable Law shall prevail. Any subsequent amendment or modification to the Applicable Law shall automatically apply to this Policy.