Enterprise Risk Management Framework Policy

1. INTRODUCTION

"Integrating enterprise risk management practices throughout INOXCVA improves decision-making in governance, strategy, objective-setting, and day-to-day operations. It helps to enhance performance by more closely linking strategy and business objectives to risk. The diligence required to integrate enterprise risk management provides company with a clear path to creating, preserving, and realizing value."

While departmental operational risk assessments are crucial, INOX India Limited ("INOXCVA") can unlock a new level of resilience by embracing Enterprise Risk Management (ERM). ERM empowers INOXCVA to proactively identify and assess enterprise-wide threats, ensuring they don't derail overall strategic goals. By gaining a comprehensive view of potential risks, INOXCVA can prioritize effectively and allocate resources strategically to safeguard its future success.

This robust approach necessitates a practical, sustainable, and user-friendly risk assessment process. By implementing such a system, INOXCVA can transform risk management from a reactive exercise to a proactive cornerstone of achieving its long-term vision.

2. CONTEXT

- This document lays down the framework of Risk Management at INOXCVA and defines the policy for the same.
- This policy covers all four plants of INOXCVA including:
  1. Kandla (KSEZ unit)
  2. Savli
  3. Silvassa
  4. Kalol
- This document shall be under the authority of the Audit Committee and/or the Board of Directors of the Company. It seeks to identify risks inherent in any business operations of the Company and lays down the mitigation methods which are periodically reviewed and modified in a manner commensurate with the size and complexity of the business.

a) Objective

To define a common framework to be applied by business management and other personnel that identifies potential events that may affect the Company, manages the associated risks and opportunities, and provides reasonable assurance that enterprise objectives are achieved. This can be further granulated into the following:

- Ensure that all the current and future material risk exposures to INOXCVA are identified, assessed, quantified, appropriately mitigated, minimized, and managed i.e. to ensure adequate systems for risk management.
- To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.
- To create awareness among the employees to assess risks continuously & develop risk mitigation plans in the interest of the Company.
- Enhanced performance.

b) Regulatory

This framework complies with the requirements of the Risk Management Framework of following regulatory requirements:

A. Companies Act, 2013:

1. Provisions of the Section 134(3)

"There shall be attached to financial statements laid before a company in general meeting, a report by its Board of Directors, which shall include—

(n) a statement indicating the development and implementation of a **risk management** policy for the Company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company."

2. Section 177(4) stipulates:
"Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, inter alia, include, —
(vii) Evaluation of internal financial controls and **risk management** systems."

3. Schedule IV [Section 149(8)]: Code for Independent Directors:
II. Role and functions:
"The independent directors shall:
(1) help in bringing an independent judgment to bear on the Board's deliberations, especially on issues of **risk management**
(4) satisfy themselves that the systems of risk management are robust and defensible."

B. Securities and Exchange Board of India (SEBI) Regulations:

1) SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, mandates listed companies to establish a framework for **risk management** and disclose the same in their annual reports.

2) Regulation 17(9) requires the board of directors to lay down the framework for **risk management**.

C. Risk Management Committee as per Listing Regulations of SEBI

1) **Composition of the RMC:** The RMC shall consist of such members as may be prescribed under Listing Regulations from time to time.
2) **Meetings of the RMC:** The RMC is to meet at such intervals as may be prescribed under the Listing Regulations from time to time.
3) **Disclosure in Annual Report:** Listed companies are required to disclose information about the risk management policies and the composition and functioning of the risk management committee in their annual reports and corporate governance reports.

3. FRAMEWORK

a) Definition of ERM

Enterprise risk management at INOXCVA is derived from the COSO ERM – Aligning Risk with Strategy and Performance 2017 framework established by a committee of sponsoring organizations. Accordingly, Enterprise Risk Management is:

"The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value."

b) Components of ERM

1. **Risk Governance & Culture***:* The company has an elaborate risk management process which is formulated based on the principles of business risk assessment, operational controls, and compliance with various policies. The company proactively identifies and systematically resolves all the major risks. The Board, through the annual report, in the management discussion

and analysis section of the Board's Report, communicates the major risks pertaining to the business of the company to all the stakeholders. The Company also demonstrates the highest commitment to Integrity and Independence of its Board, management and staff by laying down an exhaustive code of conduct covering Ethical Conduct, Conflict of Interest, Compliance with applicable laws, etc.

2. **Risk, Strategy & Objective Setting**: INOXCVA follows Risk Governance by embedding Risk into Strategic planning and day-to-day operations of the Company. Functional leaders identify internal and external risks with the help of external professionals which are then reviewed by the Audit Committee and the Board.

3. **Risk in Execution** – INOXCVA maintains a comprehensive risk register that captures all the risks faced by it. Further, these risks and responses are classified into four factors such as impact, likelihood, vulnerability and Speed of Onset of Action. Also, INOXCVA has defined its Risk appetite in this framework (Refer to section 6 Risk Appetite). Any risk having a net exposure greater than the risk appetite will be deliberated at the Audit Committee level.

4. **Risk Information, Communication & Reporting** – Communication of information is a continual and essentially core function of the business. INOXCVA has encouraged the leverage of information systems to capture, process, and manage data and information. Management reviews the risk culture using qualitative and quantitative information from internal and external factors to assess the performance of the business and report it to the stakeholders of the business.

5. **Monitoring Enterprise Risk Management Performance** – Audit committees that report to the board are in charge of monitoring the ERM performance. During their quarterly meetings, all the responses to all the risks, which are above the Risk Appetite are being deliberated between the management and the Audit Committee.

c) Risk Escalation Matrix

Risk Classification	Addressed at Which level	Roles and Responsibilities
Within Risk Appetite	Head of Department	1. Identify and report risk to the Head of Department. 2. Timely and accurate report of all incidents. 3. Identify future risks, evaluate the criticality of the risk, and submit the same to the Head of Department.
Above Risk Appetite	Head of Department and Chief Executive Officer	1. To implement all Risk management policies for all Operational Risks. 2. To report any Risks to the appropriate Forum as per the Risk Escalation Matrix. 3. Implement the decisions of the RMC with respect to Operational Risks;

Above Risk Appetite & "Very High" (Rating 5 on the Onset Scale)	Chief Executive Officer and Director	1. To implement all Risk Management Policies for all Operational Risks. 2. To report any Risks to the appropriate Forum as per the Risk Escalation Matrix. 3. Implement the decisions of the RMC with respect to Operational Risks
Above Risk Appetite & "Very High" (Rating 5 on the Vulnerability Scale).	Board / Audit Committee / Risk Management Committee	RMC to carry out the roles and responsibilities as prescribed under the Act and the Listing Regulations, including under Para C of Part D of Schedule II.

➢ Addition/Deletion of Risks

- The Audit Committee and/or the Board of Directors of the company shall be the sole custodian of the Risk management framework.
- All new risks will be identified and classified as per the section "Identification and Classification of risk".
- The Departmental Heads shall propose such risks to be added to the risk register to the Chief Executive Officer.
- Upon its Approval, the Chief Executive Officer ("CEO") shall revise the risk register accordingly.
- The Head of the Department is responsible for re-verifying the Classification and Responses to risks mentioned in the Risk Register.

➢ Revision

- This framework policy will be placed to the Risk Management Committee of the company on annual basis for revisions to it, if any.
- Revisions adopted by the Risk Management Committee shall be incorporated in this document by the Company Secretary.
- Risks as per the Risk Register shall be revised in terms of their classification, measurement, and response on annual basis.

4. RISK DEFINITION & MEASUREMENT

A.) Definition

"The possibility that events will occur and affect the achievements of strategy and business objective "

Thus,

1. Events, having positive (opportunity) and negative (threat) outcomes are covered in the definition.
2. Risk is a multiplier between the occurrences (likelihood) and the effect (impact).
3. Risk is different from uncertainty. While uncertainty is a state of not knowing how potential events may or may not occur, risk is a possibility that event will occur.

Therefore, Value is a function of Risk and Return, every decision either increases, decreases, or erodes the value.

B.) Measurement

"Risk will be measured on a annual basis using residual techniques".

Level of Risk

- Risks are measured at two levels, Inherent and Residual risk.
- Inherent risks are the risk to an entity in the absence of any actions by the management it might take to alter either the risk likelihood or impact.
- Residual Risk: Risk remaining after management response to the risk.

Methods of Measurement

- There are two methods of measuring risk: Qualitative and Quantitative
- Qualitative: Assessment of each risk and opportunity according to descriptive scales, for example (Very, High, Medium, and Low).
- Quantitative: Assessment of risk and opportunity according to numbers, for example (5 for Very high, 4 for high).

5. RISK IDENTIFICATION & CLASSIFICATION

A.) Risk Identification

a) Each Risk shall be reported by any level of management using the Event Sheet to the Head of the Department.
b) The Head of the Department shall forward the sheet to the concerned CEO of the company who shall assign:

- Risk Grades
- Risk Response

c) CEO shall decide on whether the risk merits inclusion of the same in the risk register and should be presented to the Audit Committee.
d) Accordingly, CEO shall present the risk to the Audit committee.

B.) Risk Classification

B1) Risks will be grouped into five categories.

- Strategic,
- Operational,
- Compliance,
- Financial and Reporting
- Information Technology

Examples of Risks

Types of Risks	
Strategic Risks	Reduction in business vitality (due to changes in business strategy, customer spending patterns, product discovery & development, changing technology, etc.)
	Loss of intellectual property & trade secrets
	Competition for talent
	Negative impact to reputation/loss of trust
	Risk on Account of Global Pandemics such as Covid-19, etc.
Operational Risks	Disruption to product supply
	Counterfeiting
	Inefficient use of resources/increased product cost
	Physical property/damage/disruption
	Loan repayment schedules not adhered to
Compliance Risks	Violation of laws or regulations governing areas such as:
	Environmental
	Employee health & safety
	Product quality/safety issues

	Local tax and Statutory Laws
Financial and Reporting Risks	Currency exchange, funding & cash flow, credit risk
	Financial misstatement (including violation of the Companies Act, 2013 and Listing Regulations
Information Technology	Exposure to cyber threats such as data breaches, ransomware attacks, and malware infections, potentially leads to data loss, operational disruptions, and financial losses.
	Exposure to vulnerabilities in software applications or systems leads to exploitation by hackers or malicious actors, and compromising the integrity, confidentiality, and availability of data.
	Failure to comply with data privacy regulations such as GDPR or CCPA, resulting in legal penalties, reputational damage, and loss of customer trust.

B2) Each Risk will also be assessed and graded into four parameters.

1) Likelihood
2) Impact
3) Vulnerability
4) Speed of Onset

B3) Each of the parameters mentioned above shall be graded from one to five, one being the lowest severity. Inherent Risk shall be arrived at by multiplying the score of Likelihood with the score of Impact. While each risk will have separate categorizations for Vulnerability and Impact

B4) Impact Scale

Rating	Descriptor	Parameters
5	Extreme	Financial loss of Rs. 10 crore or more
		International long-term negative media coverage; game-changing loss of market share
		Significant prosecution and fines, litigation including class action
		Significant injuries or fatalities to employees or customers
		Multiple senior leaders separation
4	Major	The financial loss of Rs. 7.5 to 10 crore or more
		National long-term negative media coverage; significant loss of market share
		Report to regulator requiring major project for corrective action

		Limited in-patient care is required for employees or third parties, such as customers or vendors
		Some senior managers exit, high turnover of experienced staff, not perceived as the employer of choice
3	Moderate	Financial loss of Rs. 5 to 7.5 crore or more
		National short-term negative media coverage
		Report of the breach to the regulator with the immediate correction to be implemented
		Widespread staff morale problems and high turnover
2	Minor	The financial loss of Rs. 2.5 to 5 crore or more
		Local reputational damage
		Minor injuries to employees or customers
		General staff morale problems and increase in employee turnover
1	Incidental	The financial loss of Rs. 2.5 crore or less
		Local media attention quickly remedied
		Issues not reportable to regulator; Isolated staff dissatisfaction

B5) Likelihood Scale

Annual Frequency		
Rating	**Descriptor**	**Occurrence**
5	Frequent	Up to once in 1 year or more
4	Likely	Once in 1 year up to once in 2 years
3	Possible	Once in 2 years up to once in 3 years
2	Unlikely	Once in 3 years up to once in 5 years
1	Rare	Once in 5 years or more

B6) Speed of Onset Scale

Speed of Onset Scale		
Rating	**Descriptor**	**Occurrence**
5	Very High	Very rapid onset, little or no warning, instantaneous
4	High	Onset occurs in a matter of days to a few weeks
3	Medium	Onset occurs in a matter of a few months
2	Low	Onset occurs in a matter of several months
1	Very Low	Very slow onset, occurs over a year or more

B7) Vulnerability Scale

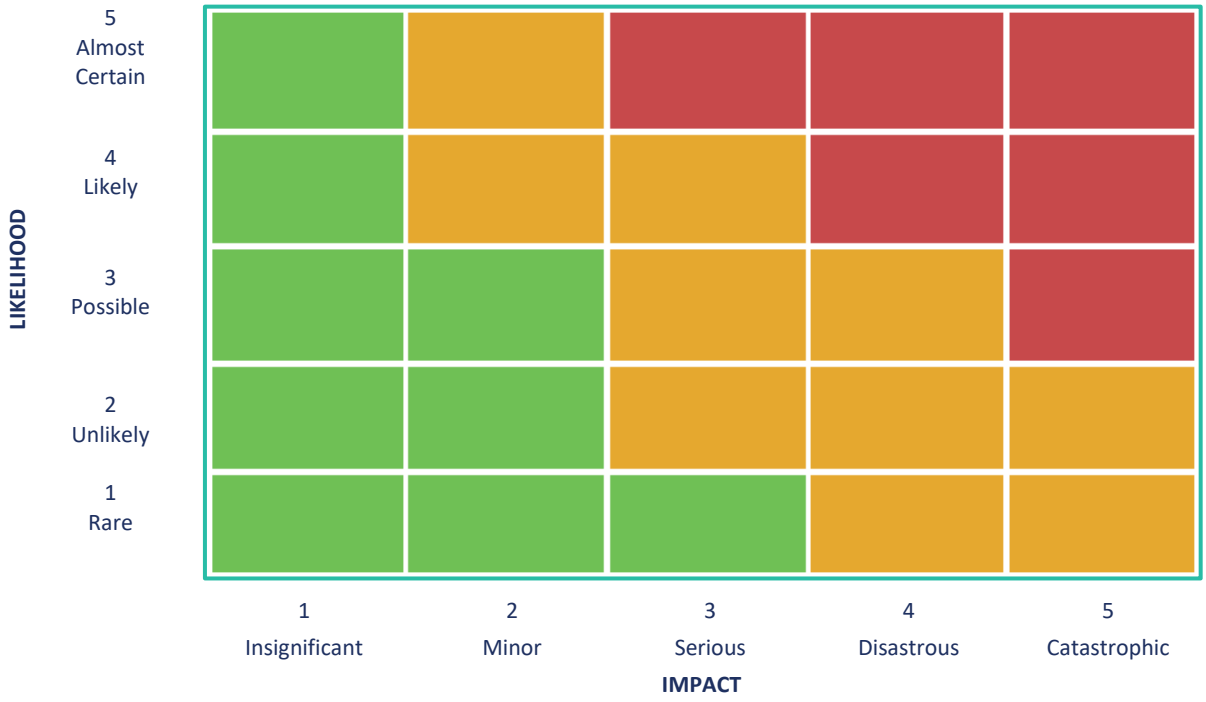
Vulnerability Scale		
5	Very High	No scenario planning was performed.
		Lack of enterprise-level/process-level capabilities to address risks.
		Responses not implemented.
		No contingency or crisis management plans are in place
4	High	Scenario planning for key strategic risks performed.
		Low enterprise-level/process-level capabilities to address risks.
		Responses partially implemented or not achieving control objectives.
		Some contingency or crisis management plans in place
3	Medium	Stress testing and sensitivity analysis of scenarios were performed.
		Medium enterprise level/process level capabilities to address risks
		Responses implemented and achieved objectives most of the time.
		Most contingency and crisis management plans are in place, and limited rehearsals
		Strategic options defined.
		Medium to high enterprise level/process level capabilities to address risks.
2	Low	Responses implemented and achieved objectives except under extreme conditions.
		Contingency and crisis management plans are in place, and some rehearsals
		Real options deployed to maximize strategic flexibility.
		High enterprise-level/process-level capabilities to address risks.
		Redundant response mechanisms are in place and regularly tested for critical risks.
1	Very Low	Contingency and crisis management plans are in place and rehearsed regularly

6. RISK APPETITE

- As explained Risk is a multiplier of likelihood and impact.
- In our case, likelihood and impact have been assigned the maximum score of 5. Therefore, the maximum possible risk would be 5 x 5 = 25 (Maximum Likelihood score x Maximum impact score)
- The Acceptance of the risk will be calculated on the Net level of score, that is the Net Risk score adjusted after the mitigation store.
- The scale of appetite is tabulated below –

Net Risk Score	Areas	Acceptance of Risk
16-25	Red	Audit Committee / Board
10-15	Orange	Chief Executive Officer and Director
6-9	Orange	Chief Executive Officer and Head of Department
Less than 6	Green	Head of Department

- Risk Matrix showing the risk appetite of the organization –



7. RISK RECORDING

The company has identified broad risks applicable to the business and recorded them in Risk Registers for the purpose of continuous monitoring. A Risk register for the INOXCVA will be prepared and approved by the Audit Committee / Board of Directors from time to time.

The Risk Register records details of all the risks identified at the beginning and during the Risk Management Process, their grading in terms of likelihood of occurring and seriousness of impact on the project, initial plans for mitigating each high-level risk, the costs and responsibilities of the prescribed mitigation strategies and subsequent results.

The recording, management, and analysis of risk incidents is a critical component of the risk management process. The other key components, being risk and control self-assessment and key risk indicators, are primarily focused on preventing risk incidents from occurring and if they do occur, to ensure the negative consequence is limited.

As part of the Risk management framework, it is important that the incident management processes are consistent and integrated into the overall framework so maximum value can be created from the sharing of information and consolidated reporting. To add, modify or delete any risk appropriate level of management has been delegated with the responsibilities.

Risk ID	Description of Risk	Type of Risk	Impact	Likelihood	Impact	Vulnerability	Speed of Onset	Overall Risk Score (Likelihood X Impact)	Date of Review	Mitigation Actions	Mitigation Score	Residual Score	Responsibility

8. Risk Response Classification

The company has developed risk response strategies based on the risks that are identified and quantified. Based on the evaluation of risk based on criteria of likelihood and Impact, the overall risk score has been derived. However, risks need to be prioritized in their order of importance for developing and deploying risk response mechanisms.

The risk response strategy is based on risk tolerance adopted by the company. Risk tolerance in terms of severity is the point above which a risk is not acceptable and below which the risk is acceptable.

The company follows a five-step process to make changes to better their approach to risk management in response to the developments in internal and external environments to address the risk management process:

1. To identify and understand the major risks.
2. To decide which risks are natural and binding to the organization.
3. To determine the capacity and appetite for identified risks.
4. To embed risk in all decisions and processes
5. To align governance and organization around risk

There are many reasons for selecting one risk strategy over another, and all these factors must be considered. Cost, Severity, or Speed of Onset are the most likely reasons for a given risk to have a high impact. Other factors may affect our choice of risk strategy. The strategy should be appropriate based on the overall criteria analyzed by the Audit Committee.

The classification of the response shall be as follows –

Tolerance / Accept Risk – One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence are low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.

Terminate / Eliminate Risk – It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing it is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

Transfer / Share the risk - Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risk associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk may also be mitigated by transferring the cost of realized risk to an insurance provider.

Treat / Mitigate the risk - Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.

Turn back - Where the probability or impact of the risk is very low then management may decide to ignore the risk.

9. BUSINESS CONTINUITY & DISASTER PLAN

Business continuity plan which refers to maintaining business functions or quickly resuming them in the event of a major disruption, in other words, a disaster management plan. The company shall formulate a business continuity plan as may be required to protect the interest of the company in the event of happening/ occurrence of any unforeseen events that may affect the business of the company. Such a business continuity plan may vary from time to time depending on the company's need and the risk management strategy being adopted by the company at such time. The business continuity plan may, among other things, focus on protecting the assets and personnel of the company in the event of a disaster event which affects day to day operations of the company's business. The business continuity plan may be reviewed and amended by the RMC from time to time, as the committee may deem fit.

Note:

- Approved by members of Risk Management Committee of the Company on 08.08.2024.