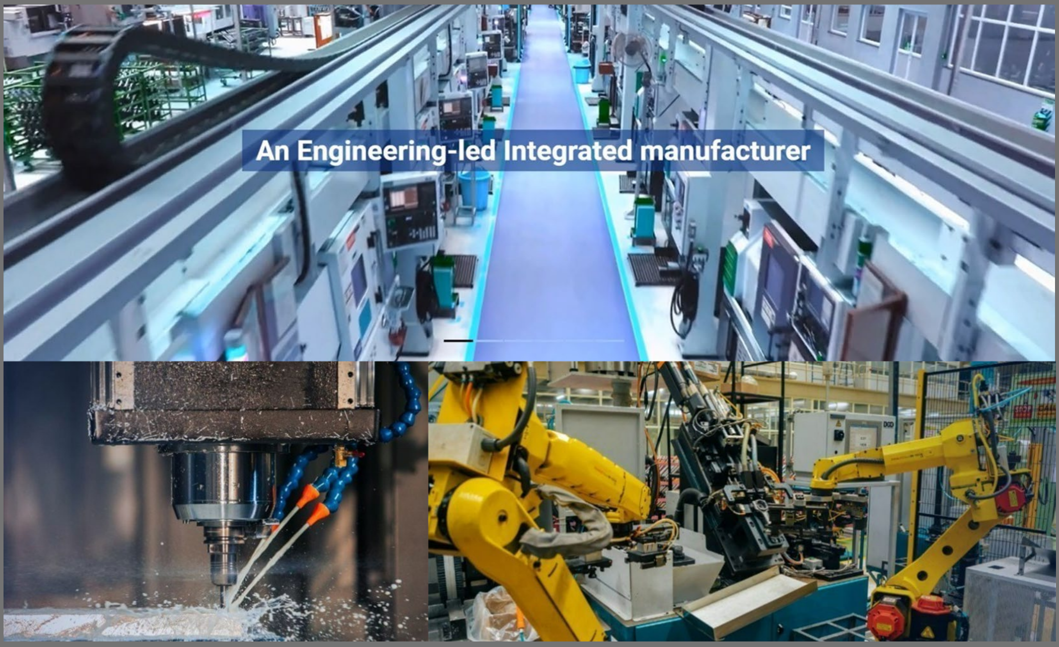
Sansera Engineering Limited

Enterprise Risk Management Policy



CONTENTS

1. INTRODUCTION

Risk Management is an integral part of an effective management practice. There is a strong correlation between risk and opportunity in all business activities. It is very important that a company identifies measures and manages the risk so as to capitalize on the opportunities to achieve its strategic objectives and goals. Rapid and continuous change in the business environment, especially in the domain of financial services, has made it necessary for management to increasingly become more risk focused

Risk management does not aim at eliminating risks completely, as that would simultaneously eliminate all chances of rewards/ opportunities. Risk management is instead focused at ensuring that these risks are known and addressed through a pragmatic and effective risk management process

Sansera Engineering Limited recognizes that profit is the reward for taking and effectively managing risk. The company will leverage Enterprise Risk Management as a part of its strategic decision-making processes. Sansera will understand its capacity to bear risk and accordingly articulate its appetite for risk.

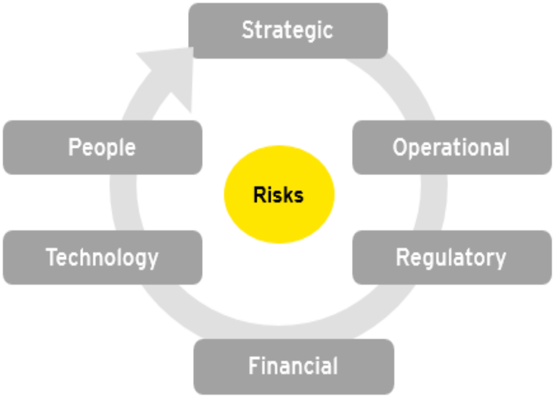
This document provides a framework for Enterprise-wide Risk Management, which typically involves identifying events or circumstances relevant to the organization's objectives, assessing them in terms of likelihood and magnitude of impact, determining a response strategy (mitigating action), and monitoring process

1.1 Risk

What is Risk?

Risk is an event that impacts business profits by way of increasing costs, decreasing revenue, or loss of market share. It is any event/non-event, the occurrence/ non-occurrence of which can adversely affect the objectives of the Company. These threats may be internal/external to the Company, may/may not be directly influenced by the Company and may arise out of routine/non-routine actions of the Company. A risk could be strategic, operational, compliance, financial, regulatory, or technological.

Classification of risks



1.2 Risk management

Why?

Risk management is at the core of the company's strategic and operational management. It is a structured process which enables the organization to identify and address the risks existing in its various activities, with the goal of achieving desired benefit from these activities. It increases the probability of success and reduces both the probability of failure and the uncertainty of achieving the organization's overall objective.

What?

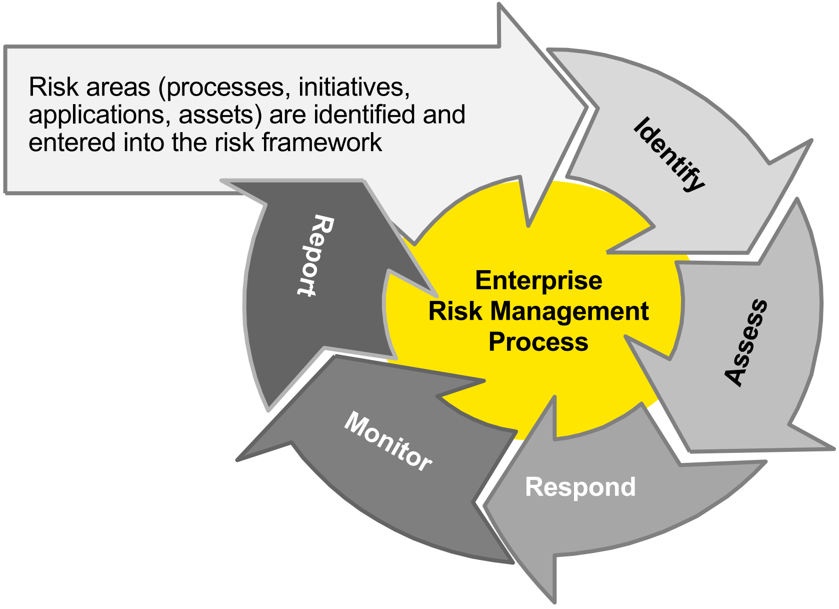
Risk Management is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on the opportunities and threats that may affect the achievement of its objectives.

1.3 Risk management framework

The components of risk management are defined by the company's business model, strategies, organizational structure, culture, risk appetite and dedicated resources. Effective risk management process requires consistent identification, prioritization, mitigation, monitoring and communication of risk issues across the full breadth of the organization. Essential to this process is its alignment with corporate direction and objectives, specifically strategic planning and annual budgeting processes. It is essential to establish acceptable risk levels which are commensurate with growth and return objectives, to ensure effective monitoring.

1.4 Risk management - Methodology

Given below is the risk management methodology at Sansera:



Risk areas (processes, initiatives, applications, assets) are identified and entered into the risk framework

Risk assessment	Prioritize risks	Mitigation plans	Monitoring and reporting
▶ Conduct interviews with key management personnel to identify risks across various functions and businesses ▶ Compile a risk register/ library describing the risks and their impact/ consequences ▶ Define risk assessment criteria	▶ Prioritize the risks based on criteria defined ▶ Conduct a risk - prioritization discussion to determine the key risks ▶ Prepare a risk map/ grid	▶ Risks with high impact and likelihood are the 'Risks that matter' ('RTMs') ▶ Assess the effectiveness of existing mitigation plans. Recommend changes/ additions, if any ▶ Assign owners and timelines for actions	▶ Report to management and Board on RTMs and status of mitigation ▶ Review the implementation status of mitigation plans as per set timelines ▶ Recommend changes, if required
Annual	**Annual**	**Annual**	**Quarterly**

Annual risk assessment

The company shall perform an annual risk assessment that coincides with its business planning exercise. The annual business plan sets a good context to identify and prioritize risks. The steps are:

- The risks are to be prioritized;
- Risks That Matter (RTMs) are to be identified;
- Improvement opportunities to enhance risk mitigation are also to be identified;
- The sum total of the existing management strategies and improvement opportunities is to be documented as a formal risk management plan for the RTM and the top RTMs along with the mitigation plans as agreed shall be presented to the Audit Committee and put up for consideration by the Board of Directors.

Quarterly risk refresh and reporting

On a quarterly basis, the risk owners formally report to Risk Management Committee on risk management within their area of operation. The purpose of this reporting is to assess how well the RTMs are being managed and if any additional risk has emerged that can adversely affect business operations. The risk report includes:

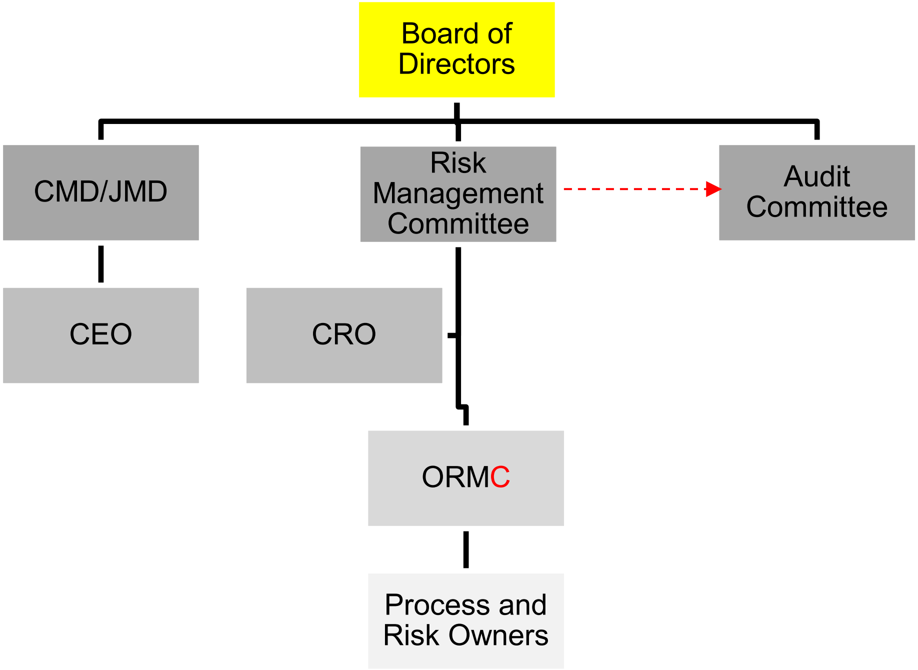
- Performance of the function on managing its RTMs in light of the mitigation strategies; and
- Identification of any additional RTMs that have emerged post the annual risk assessment, including their mitigation strategy.

The reporting process is coordinated by the Chief Risk Officer (CRO) for the company and the results shall be made available for review to the Operational Risk Management Committee (ORM).

Once approved by the ORM, the results are reviewed by the RMC and the CRO shares final results with Audit Committee and Board of Directors.

1.5 Risk Management Committee

The risk management committee is formed to facilitate the process of identifying, prioritizing and risks and forming mitigation plans. The committee is also responsible for reviewing the mitigation plans periodically and recommending changes where required.



The risk management committee is responsible for risk management to the extent of development and coordination of risk management systems and activities including:

- Monitoring the updates to the status of the corporate risk register and associated mitigation plans on a periodic basis;
- Preparing reports for Audit Committee and Board of Directors in accordance with the risk reporting protocol;
- Overseeing the successful implementation and maintenance of the company's risk management framework and procedures;
- Updating the risk management framework documents on an annual basis;
- Providing risk management advice and support (including training) to management and staff as required;
- Monitoring the implementation of risk mitigation strategies at corporate and department level for key risks;

The Operational Risk Management Committee (ORMC) shall comprise of the following members:

a. Group CEO (GCEO)
b. Chief Financial Officer (CFO)
c. Chief Risk Officer (CRO)
d. Chief Human Resource Officer (CHRO)
e. Chief Operating Officer (COO)
f. Chief Sales & Marketing Officer (CSMO)

On quarterly basis, ORMC shall present the status of Risks that Matter (“RTM”) to Risk Management Committee (RMC).

2. RISK ASSESSMENT

Risk assessment is the process of identifying and evaluating individual risks and the interrelationships between risks. It provides a systematic approach to analysis the impact of potential future event on the achievement of an organization’s objectives. The process itself typically encompasses an evaluation of available data and the application of judgement to determine the significance of potential future event and the likelihood of their occurrence. Effective risk assessment leads to formulation of risk responses. The steps involved in executing a risk assessment are:

- ► Risk Identification
- ► Update of Risk library
- ► Define Risk assessment criteria

2.1 Risk Identification

This step involves understanding and listing the potential threats that may affect the realization of the business objectives or priorities. On an annual basis, a risk library, across all products, services and functions, is prepared based on discussions with key management personnel.

Existing risk libraries and management reports serve as a baseline for this exercise. This risk profile is revisited on an annual basis by the Risk Management Committee to identify any new risk event that can adversely impact business objectives.

2.2 Risk Library

Risks that are identified are documented in a standard risk library template (refer template 7.2). The risk library details the risk and its impact/ consequence. The quality and completeness of the risk identification is the responsibility of the Risk Co-coordinator.

2.3 Risk assessment criteria

A risk prioritization criterion has been developed based on the risk appetite of the company. The same is further based on:

a. **Impact** – The extent to which the inherent risk, if realized, would impact the organization. Factors that may help define the impact rating may include financial effect, damage to the assets, reputation impacts, ability to achieve key objectives.

b. **Likelihood of occurrence** - The probability of an inherent risk occurring over a pre-defined time-period. In most instances, this is set at one year but can be adjusted to be aligned with the company’s planning horizon. In some cases, frequency of occurrence may be considered as well.

c. **Resilience** – Activities established by management to mitigate risk and may include specific monitoring activities, policies, procedures, information technology controls, physical restrictions, authorizations and other activities. It is the extent to which management and control activities are effectively designed, operated and aligned to risks that mitigates either the impact or likelihood of an inherent risk occurring.

On an annual basis, the risk management committee assesses the relevance for the defined risk assessment criteria. Risk assessment criteria has been developed based on management's risk appetite and risk tolerance

a. **Risk Appetite** – The level of risk executive management and the Board are willing to accept on an aggregate basis in relation to strategic and business objectives is considered the organization's 'Risk Appetite'. The risk appetite is set in alignment with the impact and likelihood ratings to determine how significant a risk the organization is able and willing to accept. Risk appetite is encompassed in practice through policy, guidelines and procedures and is to be considered in relation to overall growth and return on investment goals from a strategic objective perspective.

b. **Risk tolerance** – The level of risk, executive management and the Board are willing to accept to variation and variability around specific business objectives is considered the organization's 'Risk Tolerance'. Risk tolerances are quantified as ranges of deviation from goals or objectives, most often measured as performance against financial targets. The organization's tolerance for risk relates to the degree to which performance can deviate from the expected outcome for a specific goal or objective and is still considered within an acceptable range from a risk perspective. Tolerances must be aligned to the evaluation of risk management and control activities and must be set in consideration of risk appetite to determine boundaries of acceptable risk management performance

For the detailed risk assessment criteria, please refer to annexure 7.3.

Objective	Identify and compile the potential threats to the business and its operations
Responsibility	Business Head for respective business Compiled by: Chief Risk Officer (CRO) Reviewed by: Risk Management Committee
Frequency	Annual update to risk library Update to Risk assessment criteria
Output	Risk library profiling the risks for the business Updated Risk assessment criteria
Enablers	Risk Library template Risk assessment criteria

3. RISK PRIORITIZATION

This step involves identifying and selecting critical risks from the risk library. ***Risk assessment is performed based on impact and likelihood*** (as defined in section – Risk assessment criteria)***.*** This allows the business to focus on the most important risks, '**Risks That Matter'** (RTMs).

A risk prioritization criterion has been developed based on the risk appetite of the company. A voting workshop would be conducted wherein each member of the Risk Management Committee would evaluate each risk as per this criterion. After collation of the responses, risks are ranked and RTMs are identified.

3.1 Risk Ranking

Each of the risks are ranked based on:

- ► **Inherent risk** – The exposure of a risk that is intrinsic to the business in the current environment before the consideration of risk management and control activities have been designed and implemented to specifically manage a given risk. Inherent risk are classified as High, Medium and Low
- ► **Residual risk** – The exposure to a risk remaining after considering the effect of the existing risk management and control activities i.e. inherent risk offset by the aggregate impact of risk management activities / resilience equates to residual risk. Residual risks are classified as Monitor (controls), monitor (risks), Improve, Accept.

Each member of the Risk Management Committee, rates each risk, based on impact, likelihood, and resilience. Thus, each risk is given a score which is the product of impact, likelihood, and resilience. Thus, for example,

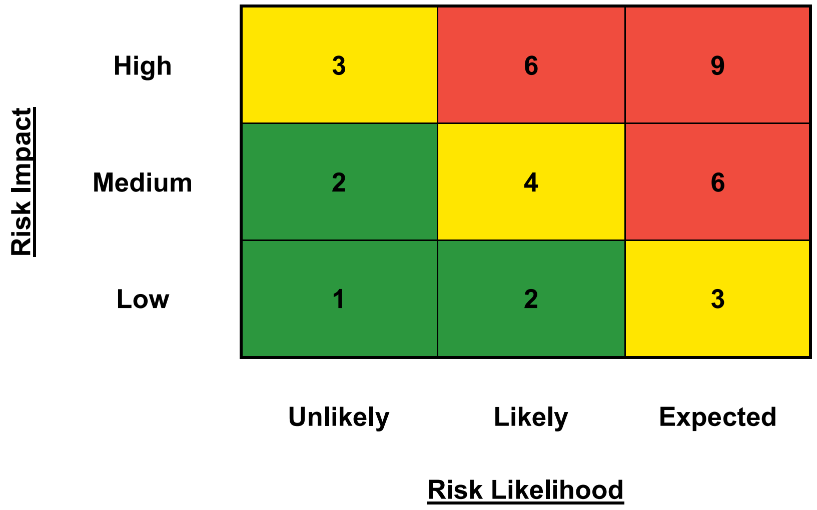
- a critical risk, which has a high likelihood of occurrence and non-existent mitigation plan would get a score of 27 (Impact: 3 x Likelihood: 3 X Resilience 3).
- Similarly, a high impact risk, whose occurrence is possible but for which the company has an effective mitigation plan would be assigned a score of 9 (Impact: 3 x Likelihood: 3 x Resilience: 1).

The scores of individual members are averaged, to arrive at group score for each risk. The risks are then ranked in descending order. Risks with high score are more important than risks with low score. The top 12 risks are the Risks that Matter (High Risks). Next 25-30 risks are classified as moderate and the balance treated as low risk events

3.2 Risk Map

A risk heat map is a tool used to present the results of a risk assessment process visually and in a meaningful and concise way. Illustrative maps are given below:

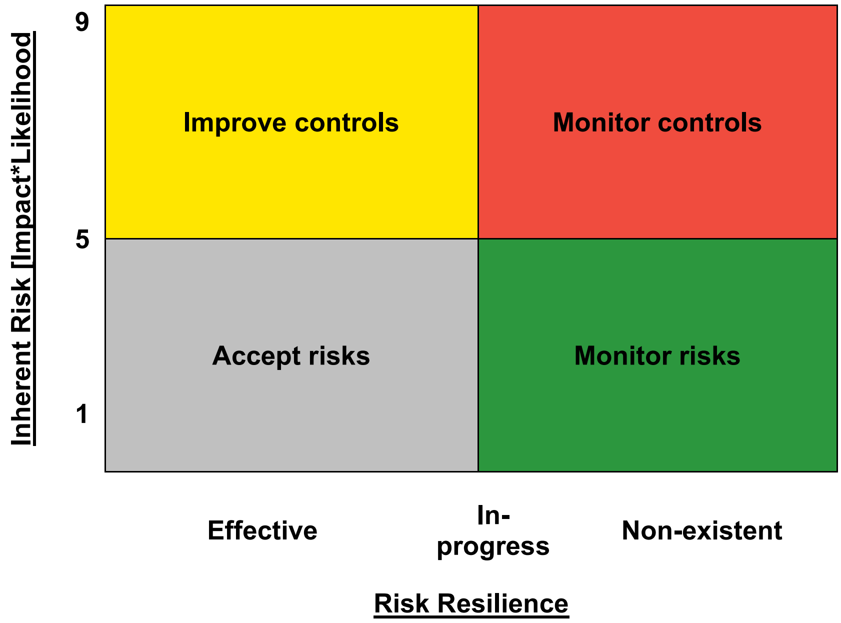
INHERENT RISK



Risk Impact	Unlikely	Likely	Expected
High	3	6	9
Medium	2	4	6
Low	1	2	3

Risk Likelihood

RESIDUAL RISK



Inherent Risk [Impact*Likelihood]	Effective / In-progress	In-progress / Non-existent
9–5	Improve controls	Monitor controls
5–1	Accept risks	Monitor risks

Risk Resilience

Objective	Identify the critical risks that can adversely impact business

	operations or the Company
Responsibility	*Prepared by*: Responded by each Business unit/Function Head *Compiled by*: Chief Risk Officer (CRO); Annually *Reviewed by:* Risk Management Committee / Board of Directors
Frequency	Annual prioritization
Output	Prioritized Risks That Matter (‘RTM’) Risk Map
Enablers	Risk Prioritization criteria Risk Library Voting exercise

4. RISK MITIGATION

This step involves preparing mitigation plans for managing the RTMs and restricting their impact to an acceptable level. A *risk owner* is assigned to each RTM in this phase. A risk owner is responsible for the co-development, implementation and reporting on the agreed mitigation plans to the Risk Coordinator / Board.

The entire process is broken down into the following activities for a Risk Owner:

a. Assess the existing processes and activities presently undertaken to address the risks
b. Identify any gaps in the existing control environment
c. Design additional mitigation strategies to adequately address the risk
d. Document the mitigation plans (with timelines), including existing and proposed activities

Objective	Identify the management response plan for addressing the Risks That Matter
Responsibility	*Prepared by*: Process Owners/ Risk Coordinators *Compiled by*: Chief Risk Officer (CRO) *Approved / Reviewed by:* Risk Management Committee
Frequency	Annual preparation and assignment of the mitigation plans Periodic review on status of implementation plans (based on risk classification) Update existing plans with additional steps (if needed)
Output	Mitigation plan with timelines Periodic status update reports
Enablers	Risk Mitigation plan template

5. MONITORING AND REPORTING PROCEDURES

On a monthly basis, the risk coordinators shall report on the status of mitigation plans to the Operational Risk Management (ORM) committee on the risks that matter (RTM's). The Operational risk committee shall review the status of mitigation, seek appropriate clarification and share status to the Risk Management Committee (RMC) / Board of Directors.
On a quarterly basis, RMC shall review the RTM status identified by ORM.
Further, the risk committee shall report the consolidated status of risks to the board directors (see templates for reporting in Annexure – 7).

Based on feedback received from the board of directors, appropriate changes shall be suggested to the risk owners for mitigation actions.

6. ROLES AND RESPONSIBILITIES

R - Responsible
A – Accountable
C – Consulted
I – Informed

Process	**Board of Directors**	**ORM**	**CRO**	**Risk Coordinators / Process owner**	**Internal audit**	**ORMC**
Risk identification	C	R,A	R,A	C	I	C
Risk voting workshops	I	C	R,A	A		I
Risk assessment criteria	I	C	R,A	I		C
Maintenance of Risk register		A	R	C	I	
Prioritizing risks	I	C	R, A		I	R
Identification of mitigation action	C			R, A	I	I
Periodic reporting on status of risks	I	A	R	C	I	I

7. Annexures

7.1 Reporting on implementation status of mitigation plans for Risks that Matter (RTMs)

Risk Number: XX

Financial Year: XX **Quarter**: XX
Date: XX/XX/XXXX

A. Details of Identified Risk

Risk Category	Risk Description	Impact	Likelihood	Resilience

B. Details of Mitigation Plans

Current State	Planned Actions	Action Owner	Due Date

Additional comments (E.g., Supporting Document Reference):

____

____

Comments by Risk Management Committee:

____

____

Comments by Board of Directors:

____

____

7.2 Risk Library template

Risk No.	Risk Group	Risk Description	Mitigating factors	Impact	Likelihood	Gross Risk	Resilience	Risk Rating*	RTM (yes/no)
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									

***Risk rating - RTM / High / Medium / Low**

7.3 Risk assessment criteria

Impact	Operational	Financials	Compliance	Technology
	Effect on operations of the business	Effect on profit/ revenue	Regulatory compliance	Effect on system availability for business operations
High	• Violation of Code of conduct and gaps leading to potential frauds/ unethical practices • Inability to achieve business objectives	• Financial exposure / monetary loss is above 0.25% of turnover	• Non-compliance which has direct impact on the Directors and Officers (e.g.: disqualification or imprisonment) or Offences which may lead to loss of operating licenses	• Unavailability of systems leading to ongoing business disruptions over 3 days
Medium	• Constrained ability to achieve business objectives • Departmental goals, plans, roles and responsibilities, SOPs are not defined/ inadequate leading to inconsistencies/ inefficiencies/ wastages/ errors	• Financial exposure / monetary loss is between 0.1-0.25% of turnover	• Regulatory offences that result in penalties or fines (> INR 1 Mn), require responding to notices or personal appearance by employees	• IT systems not scalable to meet near term requirements requiring investments in fresh infrastructure/ERP • Loss of systems leading to business disruption of more than 1 day up to 3 days
Low	• Moderate/limited impact on achievement of business objectives • Non- compliance to internal procedures leading to unauthorized transactions, inefficiencies/ wastages. • Departmental goals, plans, roles and responsibilities, SOPs are not defined/inadequate, or SOPs are not defined but a consistent process is followed	• Financial exposure / monetary loss is lower than 0.1% of turnover	• Delays, offences which involve no financial implication and can be regularized by payment of interest/submission of documents (INR 0.5 Mn to 1 Mn) • Improvements to the business processes for governing compliances	• Present IT systems need customization, change in configuration/access to mitigate risks and meet current business requirements. • Loss of systems leading to disruption of business up to 1 day

	People	Information security	Brand/ reputation	Strategy
Impact	Effect on retention & productivity	Effect on Data integrity & Confidentiality	Effect on brand reputation	Effect on strategic implementation
High	• Inability to retain significant number of key management personnel a) Overall attrition > 25% b) C-Suite->20%	• Loss/leakage of unpublished sensitive information (UPSI) to unauthorised personnel outside the company	• Loss of brand reputation or erosion of market capital above 5 %	• Unable to achieve key business objectives • Impact causes inefficiencies or missing possible efficiency gains target by more than 20% • Not achieving desired operation and financial targets by more than 15%
Medium	• High attrition in medium/ lower-level management a) Overall attrition: 10-25% b) C-Suite: 10-20%	• Loss/leakage of confidential operational information to unauthorised personnel within the company	• Adverse publicity, localized to a state/region and or erosion of market capital between 1- 5 %	• Disruption of normal operations • Impact causes inefficiencies or missing possible efficiency gains target between 10-20% • Not achieving desired operation and financial targets between 10-15%
Low	• Moderate/ low attrition in medium/ lower levels a) Overall attrition: <10% b) C-Suite: <10%	• Loss/sharing of sensitive confidential information to inappropriate internal personnel leading to employee discontent/financial risk • Sharing/loss of non-confidential information which may result in discontent amongst few employees/vendors/channel partners	• Adverse publicity, localized to a city / within the organization • Loss of credibility with vendors/suppliers	• Able to deal with matter in short term within normal business activities • Impact causes inefficiencies by less than 10% • Not achieving desired operation and financial targets by less than 10%

	Qualitative Rating	Description	Quantitative rating
Likelihood	Likely (3)	Might occur at sometime	> 75 %
	Possible (2)	May occur on exceptional basis	25% - 50%
	Unlikely (1)	Might not occur or rarely	<25%

	Qualitative Rating	Description
Resilience	Non-existent (3)	No mitigation plan in place to prevent risk occurrence
	Ineffective (2)	Mitigation plans not effective in controlling risk
	Effective (1)	Mitigation plans involve stringent approval & reporting norms with responsibility for execution duly mapped to various management levels ensuring adequate control over risk occurrence