

eClerx

Risk Management Policy



Project	Risk Management Policy
Company	eClerx Services Ltd.
Prepared by	Legal & Secretarial

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

This document is copyright protected in content, presentation, and intellectual origin, except where noted otherwise. You may not modify, remove, augment, add to, publish, transmit, participate in the transfer or sale of, create derivative works from, or in any way exploit any of the elements of this document, in whole or in part without prior written permission from eClerx Services Ltd. © 2025-2026.

Table of Contents

1.	Introduction	5
1.1.	Objective of the Policy	5
1.2.	Definitions	5
1.3.	Effective Date.....	6
2.	Legislation and Applicability	7
3.	Risk Management Committee.....	8
3.1.	Guiding principle for Constitution of the Risk Management Committee	8
3.2.	Committee Members and Quorum for the meeting	8
3.3.	Functions of Risk Management Committee	8
4.	Risk Management Framework (Enterprise Wide)	10
4.1.	Methodology for Risk Management	10
5.	Training and Reporting.....	13
6.	Communication and Consultation	14
7.	Record-keeping	15
8.	Responsibility	16
9.	Amendment.....	17
10.	Annexure 1	18
11.	Annexure 2	19

List of Tables

Table 1: Risk Category and Instances 10

Table 2: Risk score 11

Table 3:Risk Register 19

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

1. Introduction

eClerx Services Limited (“the Company”) considers risk management to be a core component of the management of the Company and understands the Company’s ability to identify and address risk is central to achieving its corporate objectives. The Company’s Risk Management Policy (‘the Policy’) outlines the program implemented by the Company to ensure appropriate risk management within its system and culture. The policy is formulated in compliance with the provisions of the Companies Act, 2013 (‘the Act’) and Regulation 17(9)(b) of the SEBI (Listing Obligations and Disclosure Requirements), Regulations, 2015 (‘the LODR Regulations’).

1.1. Objective of the Policy

Risk is an inherent aspect of the dynamic business environment. The policy helps organizations to put in place effective framework for taking informed decisions about risks. It maximize opportunities and minimize the adverse consequences of risk on business objectives of the Company and assists in decision making processes that will minimize potential losses, improve the management of uncertainty and the approach to new opportunities, thereby helping the Company to achieve its objectives.

The key objectives of this policy are:

- Safeguard the Company assets, interests and interest of all stakeholders by identifying, assessing and mitigating various risks.
- Lay down a framework for identification, measurement, evaluation, mitigation & reporting of various risks.
- Evolve the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects, which the business and operations of the Company are exposed to.
- Balance between the cost of managing risk and the anticipated benefits.
- To create awareness among the employees to assess risks on a continuous basis & develop risk mitigation plans in the interest of the Company.

1.2. Definitions

In this Policy unless the context otherwise requires:

1. ‘Act’ means Companies Act, 2013 and rules framed thereunder.
2. ‘Board of Directors’ or ‘Board’, in relation to the Company, means the collective body of the Directors of the Company.
3. ‘Committee’ means Risk Management Committee.
4. ‘Audit Committee’ means Committee constituted as per provisions of the Act and the LODR Regulations.
5. ‘CRO’ means Chief Risk Officer of the Company i.e. CFO (Chief Financial Officer) appointed asCRO by the Board.
6. ‘Directors’ means Directors of the Company as appointed under the provision of the Act.
7. ‘Independent Director’ means a director referred to in Section 149(6) of the Act and the relevant Regulations of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.

8. 'Policy' means Risk Management Policy.
9. 'Risk' is an event which can prevent, hinder and fail to further or otherwise obstruct the enterprise in achieving its objectives. It can cause financial disadvantage, for example, additional costs or loss of funds or assets. Risk can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of likelihood of occurrence of an event and the probable impact of such occurrence to an enterprise.
10. 'Risk Assessment' is the overall process of risk analysis and evaluation.
11. 'Risk Management' is the culture, processes and structures that are directed towards the effective management of potential risks and their adverse effects.
12. 'Risk Management Process' is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, mitigating, monitoring and communicating risk.
13. 'Risk Owner' is the Department head (or other Associate Principle and above designated employee as may be relevant), who will be responsible for strategic risk management within areas under his/her control including the devolution of the risk management process to operational managers. Each risk should be owned by a specified person ('Risk Owner'), who should effectively monitor & ensure timely management of the risk.

1.3. Effective Date

The Risk Management policy was approved by the Board on March 31, 2009 which was amended on November 7, 2019, August 13, 2021, March 29, 2023, March 13, 2024 and October 24, 2025.

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

2. Legislation and Applicability

As per Companies Act, 2013

Pursuant to Section 134(3)(n) of the Act, the Board of Directors' report must include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the board may threaten the existence of the Company.

As per Section 177(4)(vii) of the Act, the Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall, interalia, include evaluation of internal financial controls and risk management systems. The Independent Directors should satisfy themselves that financial controls and the systems of risk management are robust and defensible in accordance with the Schedule IV [Part II-(4)] of the Act.

SEBI (Listing Obligation and Disclosures Requirements) Regulations, 2015

The Company through its Board of Directors shall constitute a Risk Management Committee and shall define the roles and responsibility of the Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit.

In accordance with the Schedule II [Part C-A(11)] of the LODR Regulations, Audit Committee shall evaluate internal financial controls and risk management systems of the Company.

The Policy is applicable to all the functions and departments of eClerx Services Limited.

3. Risk Management Committee

3.1. Guiding principle for Constitution of the Risk Management Committee

The Risk Management Committee shall consist of minimum three members with majority of Board of Directors including atleast one Independent Director, provided that chairperson of the Committee shall be member of the Board and any of the employee in the cadre of Associate Principal and above may be appointed as member of the Committee.

The risk management committee shall meet at least twice in a financial year to review the objectives and carry out functions as set out in the Policy. The Committee members may attend the meeting physically or via permitted audio-visual mode, subject to the provisions of the applicable Regulations. The Committee shall have the authority to ask such employee(s), senior official(s) and / or externals to attend its meeting, as it deems fit. The Company Secretary shall act as Secretary to the Committee.

3.2. Committee Members and Quorum for the meeting

The Chairperson and Members of the Committee will be decided by the Board of Directors.

The quorum for a meeting of the Risk Management Committee shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance.

3.3. Functions of Risk Management Committee

The Risk management Committee shall, *inter-alia*, perform the following functions:

1. To formulate a detailed risk management policy and monitor and oversee the implementation of the policy and the EWRM framework, including evaluating the adequacy of risk management systems. The policy shall include:
 - a. A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly ESG related risks), information, cyber security risks or any other risks as may be determined by the Committee;
 - b. Measures for risk mitigation including systems and processes for internal control of identified risks.
 - c. 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 periodically review the risk management policy, atleast once in two years, including by considering the changing industry dynamics and evolving complexity.
4. To keep the Board of Directors informed about the nature and content of its discussion, recommendations and actions to be taken;
5. The appointment, removal and terms of remuneration of the Chief Risk Officer shall be subject to review by the Risk Management Committee.
6. Periodic assessment and prioritizing of risks that affect the operations of the Company;
7. Identify and review the Company's risk appetite for various elements of risk including cyber security;
8. Review the risk management practices and recommend changes to ensure its adequacy;

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

9. Monitor the implementation of the risk mitigation plans including mitigation of cyber security risk;
10. To seek information from any employee obtain outside legal or other professional advice and secure attendance of outsider with relevant expertise, if it considers necessary.
11. Such other functions as the Board may determine from time to time.

4. Risk Management Framework (Enterprise Wide)

'Enterprise Wide Risk Management' (EWRM) framework is an organized methodology through which, efficient Risk management is ensured by the Company. Effective risk management is a factor of early identification and analysis of risks, implementation of corrective measures and continuous monitoring.

4.1. Methodology for Risk Management

Risk management is a shared responsibility. The risk management process model includes the following key activities, performed on a continuous basis:

1. Identification of Risks

This would envisage identification of the potential list of events/perils/risks/factors that could have an adverse impact on the achievement of business objectives. This is a Continuous process of Identification of Risk events that may have negative impact on the Company's ability to achieve goals. The Identification of risks, risk events and their relationship are defined on the basis of discussion with the risk owners and secondary analysis of related data, previous internal audit reports, past occurrences of such events etc. Risks can be identified under the following broad categories and mapped by risk Owners. The below list is not intended to be exhaustive and is for illustrative purposes only.

Risk Category	Instances
Strategic Risk	Competition, inadequate capacity, high dependence on a single customer/vendor
Business Risk	Project viability, Process risk, technology obsolescence/changes, development of alternative products
Finance Risk	Liquidity, credit, currency fluctuation
Environment Risk	Non-compliances to environmental regulations, risk of health to people at large
Personnel Risk	Health & safety, high attrition rate, incompetence
Operational Risk	Process bottlenecks, non-adherence to process parameters/pre-defined rules
Reputation Risk	Brand impairment, product liabilities, data or privacy breaches
Regulatory Risk	Non-compliance to statutes, change of regulations
Technology Risk	Innovation, obsolescence, cyber attacks
Political Risk	Changes in the political environment, regulation/deregulation due to changes in political environment

Table 1: Risk Category and Instances

2. Risk Analysis

Risk analysis is the determination of the existing controls and the analysis of the risks in terms of the likelihood and impact of the risk in the context of the existing controls. The analysis considers the range of likelihood of occurrence and probable impact of the risk, which are reviewed to produce an estimate level of risk.

The risks are assessed before and after the current control activities. The assessment of risks at the '**inherent level**' (before considering the current control activities) facilitates prioritization of risks. The assessment of risks at the '**residual level**' (risk that remains after considering control activities) helps to determine whether the current risk level is acceptable or requires further mitigation plan. All risks are assessed at the inherent and residual levels.

3. Risk Assessment and Categorisation

This is a comparison of estimated risk levels against pre-established criteria. This enables risks to be ranked and prioritized. The risks can be assessed by plotting them on the Risk Map (Annexure 1).

- Likelihood of Occurrence and Probable Impact of the risk will be evaluated on an annual basis.
- The result of this risk assessment should be mapped in the Risk Map, which should depict the probable impact of the risk on the Y- axis on a scale of 1-10 and the likelihood of occurrence of the risk on the X- axis on a scale of 1- 10.
- Thus, based on the results of the Risk assessment study and the judgment of the Risk Owner and the CRO each risk should be mapped in the Risk Map. The, risk map highlights the 'Risk Score' (from 1 to 100) for each risk identified in the function/department.
- Based on the risk score the risks can be classified in the following categories:

Risk Category	Score	Impact/Action Strategy
Extremely High Risk (A)	More than 60 points	Severe. Strategic/ critical risks, which need to be addressed & followed-up by the senior management /Board on a priority basis.
High Risk (B)	Between 40 to 60 points	Serious. Business risks which result in major business disruptions and need to be addressed and followed-up by senior management.
Medium Risk (C)	Between 30 to 40 points	Medium. These risks are more operational in nature and need to be primarily addressed by the concerned Department Heads, along with the Senior Management.
Low Risk (D)	Below 30 points	Insignificant. These risks fall last in the organization-wide corrective action plan considering their relative importance to the organization and thus, can be managed by the middle/lower management.

Table 2: Risk score

- The CRO should classify risks in the above category and define the range of monetary impact to ensure proper classification of risks according to the nature & size of the operations of the Company. The risks so categorized and the range of monetary impact, thereof, may be reviewed as and when required.
- CRO may identify certain risks, which cannot be quantified in monetary terms and as such not possible to rank them. In such cases, the consequences of the risk need to be evaluated. The following could be used as criteria to identify such risks:
 - Impact on fatality or irreversible disability/impairment to human life;

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

- Impact on the environment;
- Impact on the Brand Equity including public litigation.

4. Risk Treatment – Mitigation

Risk mitigation options are considered in determining the suitable risk treatment strategy. For risks categorized into 'High' and 'Extremely High' categories, the CRO with the help of Risk Owners and management would develop and implement specific risk management/mitigation plans. Low priority risks may be accepted and monitored. The CRO should evaluate avoiding risk or eliminating or radically reducing the risk by considering alternatives to current or proposed activities. The CRO would ensure adoption of the control measures to be initiated against the identified risks from the designated personnel after analyzing severity of the risk. The existing controls supporting the strategy are recorded in a 'risk register' along with the timelines for mitigating or eliminating 'High' and 'Extremely High' priority risk.

Explanation – “Risk register” The CRO should ensure compilation of a Risk Register (Annexure 2) for 'High' and 'Extremely High' priority risk in the specified format. The following should be included in the Risk Register.

- Name of the function/department
- Date of risk review
- Risk description i.e. nature of risk
- Risk indicators – an event or factor which indicates presence of a risk.
- Risk drivers - source of risk
- Impact & likelihood
- Risk score & Risk category
- Existing controls
- Risk ownership

5. Monitoring and Review

Risk management uses the output of a risk assessment and implements counter measures to reduce the risks identified to an acceptable level. It helps to oversight and review the risk management system and any changes that might affect it. Monitoring and reviewing occurs concurrently throughout the risk management process.

- The CRO is responsible for overall monitoring of the risk management processes.
- As 'Risk Owners' for the areas under their control every Department head will support the CRO for timely identification of risks and development of risk mitigation plan.

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

5. Training and Reporting

The CRO may identify the need for imparting training to Risk Owners as well as other key personnel in the organization who are involved in the process of risk assessment and management and accordingly design and implement training plan.

Reporting of 'High' and 'Extremely High' risks, their exposure and the risks mitigation plan devised by the Company shall be done to the Committee at its meeting on continuous basis having gap of not more than 210 days between 2 meetings. The committee meeting shall be convened on alternate quarterly basis and the same shall be reviewed by the Audit Committee and the Board at their respective annual meetings. The responsibility of compilation of report is entrusted with the CRO. The Risk Owners should submit quarterly report on the compliance of the risk assessment & management policy to the CRO.

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

6. Communication and Consultation

Appropriate communication and consultation with internal and external stakeholders would occur at each stage of the risk management process as well as on the process as a whole.

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

7. Record-keeping

Risk Management Plans and Risk Matrix shall be retained by the Company for a minimum period of 8 (Eight) years.

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

8. Responsibility

The CRO has overall responsibility for ensuring that this Policy complies with our legal and ethical obligations and that all those under our control comply with it. He is accountable for ensuring that a risk management system is established, implemented and maintained in accordance with this policy. The assignment of responsibilities in relation to risk management will be done by the CRO.

Risk Owners at all levels are responsible for ensuring that those reporting to them are made aware of and understand this Policy, undertake training on how to implement and adhere to it and also monitor compliance of it.

Internal and External auditors are responsible to ensure, through their periodic reviews that risk management processes are adequately followed by the company and also ensure that all statutory requirements are complied with and advise the management on new risks, if any identified during the course of audit.

Document Title: Risk Management Policy	eClerx
Template Version: 5.0	
Last Updated: October 24, 2025	

9. Amendment

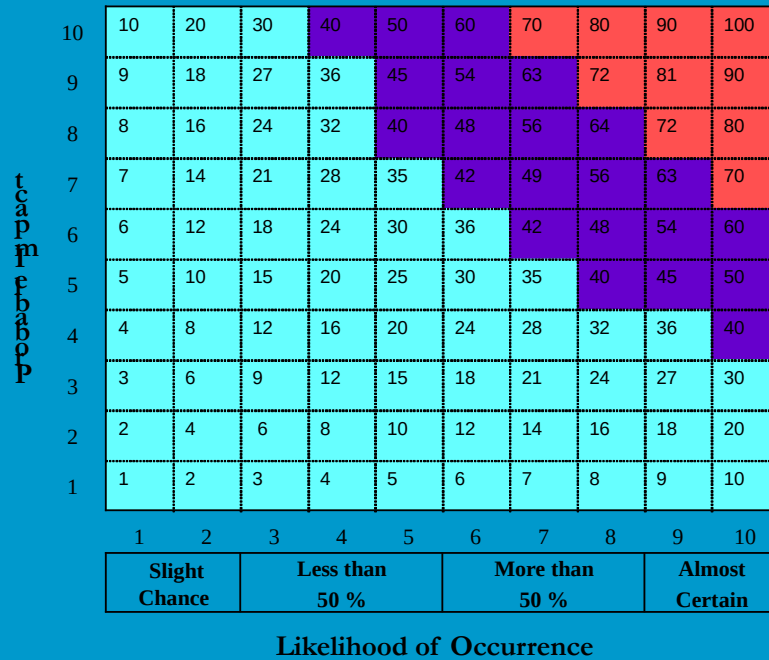
The Board of Directors on its own and/or as per the recommendations of Risk Management Committee can amend this Policy, as and when deemed fit.

In case of any amendment(s), clarification(s), circular(s) etc. issued by the relevant authorities, not being consistent with the provisions laid down under this Policy, then such amendment(s), clarification(s), circular(s) etc. shall prevail upon the provisions hereunder and this Policy shall stand amended accordingly from the effective date as laid down under such amendment(s), clarification(s), circular(s) etc.

10. Annexure 1

Annexure 1

RISK MAP



11. Annexure 2

Risk Register

Name of the Company	eClerx Services Limited	Risk Review Date:	
Function/Department		Compiled By:	Name & Date
Chief Risk Officer		Reviewed By:	Name & Date

Risk Ref.	Risk Description	Risk Score			Adequacy of existing Controls	Risk Category (A, B, C,D)	Risk Mitigation Plan Ref.
		Impact	Likelihood	Total out of 100			

Table 3:Risk Register

For ECLERX SERVICES LIMITED
Sd/-

Place: Mumbai
Date: October 24, 2025

Kapil Jain
Managing Director & Group CEO