Vivriti Capital Limited

Risk Management Policy

Version 3.0

Project/ Track Name	Vivriti Capital
Document Name	Risk Management Policy
Document No	ISP-08
Revision no	3.0
Object Type	Policy Document

Revision History						
Version	**Author**	**Date**	**Affected Sections**	**Reviewer**	**Approver**	**Approval Status**
2.0	Lakshmi Balaji	06-10-2022	All	Prasenjit Datta	ISMGC	Approved by board on 08-Nov-2022
3.0	Goutham Vaidyanathan /Lakshmi Balaji	5-10-2023	All	Prasenjit Datta		Approved by board on 03-Nov-2023

Note: This policy is the revamped version of older version (V1.x) to meet the technology, regulatory and compliance requirement.

Distribution	
Role	**Department**
All	All

Table of Contents

Important Note: 4
1. Purpose 5
2. Scope 5
3. Risk Assessment Areas and Frequency 5
3.1. Contextual Risk Assessment 5
3.2. Information Security Risk Assessment 5
3.3. Privacy Risk Assessment 5
4. Third-Party Risk Assessment 5
4.1. Co-Lending Partners 5
4.2. Other Third Parties 6
5. Risk Management Framework 6
5.1. Risk Identification 6
5.2. Risk Assessment 6
5.3. Risk Treatment 6
5.4. Roles and Responsibilities 6
6. Compliance with Standards and Regulations 6
6.1. ISO 27001 and ISO 27701 Compliance 6
6.2. Regulatory Compliance 6
7. Documentation and Records 7
7.1. Risk Assessment Records 7
8. Training and Awareness 7
8.1. Employee Training 7
9. Communication 7
9.1. Risk Communication 7
10. Review and Improvement 7
10.1. Contextual Review 7
10.2. Continuous Improvement 7
11. Conclusion 7

1. Purpose

The purpose of this Risk Management Policy is to establish a robust framework for identifying, assessing, and managing risks associated with our operations at Vivriti Capital Limited, aligning with ISO 27001 (Information Security Management) and ISO 27701 (Privacy Information Management) standards. This policy also addresses third-party risk assessment, including co-lending partners and others

2. Scope

This policy applies to all aspects of Vivriti Capital Limited's operations, including information security, data privacy, and third-party relationships. It encompasses the entire organization's risk context within the scope of work of information security and privacy, which includes:

- Information Security and Privacy program development and implementation.
- Information security and Privacy Governance.
- Information security and privacy incident response.
- User awareness on information security and privacy.
- Infrastructure and Application security assessment and VAPT.
- Information security and privacy Audit, Risk, Compliance, and reporting.

3. Risk Assessment Areas and Frequency

3.1. Contextual Risk Assessment

- Conduct a contextual risk assessment, at least annually, to evaluate the external and internal factors that may affect the NBFC. This includes changes in regulatory requirements, market dynamics, economic conditions, and emerging threats.

3.2. Information Security Risk Assessment

- Perform information security risk assessments annually or when significant changes occur. Identify risks related to information assets, data processing, access control, network security, software, and emerging technologies.

3.3. Privacy Risk Assessment

- Conduct annual privacy risk assessments in alignment with ISO 27701. Evaluate the risks associated with personal data processing, data protection measures, and compliance with data privacy regulations.

4. Third-Party Risk Assessment

4.1. Co-Lending Partners

- Evaluate the risks while onboarding a new co-lending partner. The risk assessment should be performed as per the enhanced due diligence mandated by RBI guidelines (DOR.CRE.REC.66/21.07.001/2022-23).

- Evaluate the risks associated with co-lending partnerships annually. Assess the partner's security and privacy controls, data handling practices, and contractual obligations.

4.2. Other Third Parties

- Assess the risks posed by other third parties annually or as needed. This includes vendors, service providers, and contractors who have access to your data or provide services that impact your operations. Ensure compliance with ISO 27001 and ISO 27701 standards.

5. Risk Management Framework

5.1. Risk Identification

- Identify contextual, information security, privacy, and third-party risks. Ensure a systematic approach to risk identification, considering both internal and external factors.

5.2. Risk Assessment

- Evaluate risks based on likelihood, impact, and context-specific criteria. Prioritize risks for mitigation based on business-criticality and compliance requirements.

5.3. Risk Treatment

- Develop risk treatment plans that align with business objectives. Address risks with appropriate controls, policies, and procedures. Ensure third-party risk mitigation measures are communicated and enforced.

5.4. Roles and Responsibilities

- Senior Management: Senior management is responsible for establishing and supporting the risk management framework, providing necessary resources, and ensuring compliance with ISO 27001 and ISO 27701.
- Information Security and Privacy Team: The Information Security and Privacy Team is responsible for coordinating risk assessments, developing risk treatment plans, and monitoring risk mitigation activities.
- Employees and Third Parties: All employees and third parties are responsible for reporting potential risks, following security and privacy policies, and participating in risk management activities.

6. Compliance with Standards and Regulations

6.1. ISO 27001 and ISO 27701 Compliance

- Maintain compliance with ISO 27001 and ISO 27701 standards by incorporating their principles into risk management practices and privacy information management.

6.2. Regulatory Compliance

- Stay current with financial and data privacy regulations that may impact the NBFC's operations. Ensure risk assessments and controls align with these requirements.

7. Documentation and Records

7.1. Risk Assessment Records

- Document risk assessments, treatment plans, and results. Keep records of third-party assessments, including co-lending partners and other vendors.

8. Training and Awareness

8.1. Employee Training

- Provide training to employees and relevant staff on risk management principles, security, privacy, and compliance requirements.

9. Communication

9.1. Risk Communication

- Implement a system for reporting and communicating risks within the organization. Ensure effective communication channels for third-party risk assessment results and remediation efforts.

10. Review and Improvement

10.1. Contextual Review

- Regularly review Vivriti Capital Limited's contextual risk environment and adjust risk management strategies accordingly.

10.2. Continuous Improvement

- Continuously improve risk management processes, controls, and third-party relationships to adapt to changing conditions and emerging risks.

11. Conclusion

- This Risk Management Policy is a dynamic framework designed to adapt to the evolving risk landscape of Vivriti Capital Limited. It emphasizes a context-based approach, alignment with ISO standards, and thorough third-party risk assessment practices. The policy must be reviewed and updated regularly to remain effective and compliant with changing regulatory requirements.