Version	Approval Date	Prepared By	Approved By
V2	07-Nov-2022	Info Sec	Board
V2.1	03-Nov-2023	Info Sec	Board
V2.2	07-Feb-2024	Info Sec	Board

Table of Contents

Important Note:

This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

1. Purpose

The purpose of this Risk Management Policy is to establish a context based robust framework for identifying, assessing, and managing risks associated with our operations at Vivriti Capital Limited, aligning with legal, regulatory, compliance requirements and 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 as per the RBI guidelines and master direction on IT Governance, risk, control and assurance practices, IT outsourcing activities and enhanced due diligence and technology controls/requirements on co lending partners (digital lending in particular).

3. Periodic review of IT/ Information Security/Privacy related risks

Vivriti shall review IT/Information security related risks, including the Cyber Security related risks, privacy related risks and the same shall be discussed with Risk Management Committee of the Board (RMCB) in consultation with the ITSC at least on a yearly basis.

4. IT and Information Security Risk Management Framework

- Vivriti shall establish a robust IT and Information Security Risk Management Framework covering, the following aspects:
- Implementation of comprehensive Information Security management function, internal controls and processes (including applicable insurance covers) to mitigate/ manage identified risks. The implemented controls and processes must be reviewed periodically on their efficacy in a risk environment characterized by change.
- Definition of roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Areas of possible role conflicts and accountability gaps must be specifically identified and eliminated or managed.
- Identification of critical information systems of the organization and defenses of the security environment of such systems
- Definition and implementation of necessary systems, procedures, and controls to ensure secure storage/ transmission/ processing of data/ information.

5. Risk Assessment

- The risk assessment for each information asset within Vivriti’s scope shall be guided by appropriate security standards/ IT control frameworks.

- Vivriti shall ensure that all staff members and service providers comply with the extant information security and acceptable-use policies as applicable to them.
- The organization shall review their security infrastructure and security policies at least annually, factoring in their own experiences and emerging threats and risks and take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.
- Vulnerability Assessment (VA) / Penetration Testing (PT) shall be conducted as per the VAPT policy.
- An approved Cyber Incident Response and Recovery Management procedure shall be in place and the same shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage such incidents, contain exposures and achieve timely recovery.

6. Risk Management Areas and frequency

Vivriti shall adapt to contextual risk management of all IT and Information assets that may impact its information security and privacy posture and may have business impact and reputational loss. The scope shall be as follows:

Internal risk management:

This includes risk management of

- IT and Information security/Privacy Governance
- IT infrastructure and service management
- Business continuity and disaster recovery
- Information security, cyber security and privacy
- Infrastructure security
- Software and application security
- IT services outsourcing

Partner risk management:

This includes risk management of

- The information security and privacy posture of the partner system
- The security assessment of the partner software that Vivriti may use/integrate with to carry out its business functions.
- Enhanced due diligence on co-lending partners.

Third party risk management:

This includes risk management of

- Vendors/service providers.
- New IT system software procurement/integration.
- Existing software vendors/OEM who have access to Vivriti’s data.

Risk management shall be conducted at least on an annual basis on the identified areas and the identified critical risks shall be discussed and presented to the risk management committee of the board.

7. Risk Management Framework

Vivriti shall define a risk control framework covering all areas defined under risk management areas. Then the next steps of risk management shall take place as follows:

Risk Identification:

This shall happen in multiple ways like audit, assessment, incident etc. Once the risk is identified it is documented.

Risk Assessment:

Once the risk is identified, impact assessment is conducted, and appropriate ranking is given to the risk as key/non-key. All fraud risks and any other risk which can create financial /reputational impact are categorized as key risk.

Risk Treatment:

The identified and assessed risk shall be mitigated (by applying appropriate controls), transferred (to a third party), avoided (by identifying alternatives), accepted (only if within limits).

Monitor results:

Once a decision has been made on the identified risks, the implementation is done and the same is monitored for effectiveness and maintenance of the same within the acceptable limit.

8. Roles and Responsibilities and documentation

- The IT Steering committee is responsible for implementing the policy.
- The Information Security team is responsible for conducting and driving risk management in the defined areas and periodic reporting of the identified risks to the management and risk committee.
- The IT teams/respective teams are responsible for implementing control/treatment of identified risk.
- All involved teams are responsible for incorporating lessons learnt as applicable into their function.

All risk management and assessment reports and related documentation shall be presented to the Internal Audit team or any other audit that is carried out to meet regulatory and compliance requirements.

9. Compliance with Standards and Regulations

To maintain compliance with ISO 27001 and ISO 27701 standards by incorporating their principles into risk management practices and privacy information management, and to stay current with financial and data privacy regulations that may impact the NBFC's operations measures shall be in place to ensure risk assessments and controls align with these requirements.

10. Review and Improvement

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 same shall be regularly reviewed and modified if need be and risk management strategies shall be adjusted accordingly.

11. Document review:

Review of this policy shall be done annually or upon any operational/regulatory/legal change in requirement and the same shall be done by the Info Sec team after taking inputs from the concerned.

-- End of Document --