

Vivriti Capital Limited

Governance Framework Policy

Version 3.0



Project/ Track Name	Vivriti Capital
Document Name	Governance Framework Policy
Document No	ISP-18
Revision no	3.0
Object Type	Policy Document

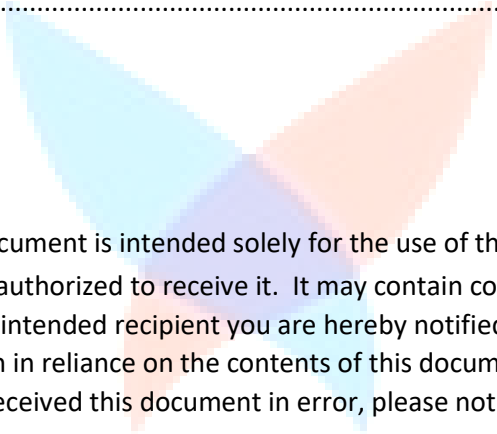
Revision History						
Version	Author	Date	Affected Sections	Reviewer	Approver	Approval Status
2.0	Lakshmi Balaji	06-10-2022	All	Prasenjit Datta	ISMGC	Approved by board on 08-Nov-2022
3.0	Goutham Vaidyanathan /Lakshmi Balaji	15-10-2023	All	Prasenjit Datta		Approved by board on 03-Nov-2023

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:	3
1. Purpose	4
2. Scope.....	4
3. Objectives	4
4. IT Governance Principles	4
5. Information Security Governance Principles	4
6. Standards and Regulations	5
7. Roles and Responsibilities.....	5
8. Review and Amendments	5
9. Conclusion.....	6



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 IT Governance Framework and Information Security Governance Policy is to establish a robust structure for managing information and IT resources in line with industry best practices, legal regulations, and the specific requirements set forth by the Reserve Bank of India (RBI) for Non-Banking Financial Companies (NBFC).

2. Scope

This framework and policy apply to all IT and Information Security operations, activities, personnel, and third-party service providers associated with Vivriti Capital Limited.

3. Objectives

To ensure:

- Alignment of IT strategy with business goals.
- Information Security and Privacy Risk management is integrated into business processes.
- Effective and efficient use of IT resources.
- Compliance with applicable laws, standards, and regulatory requirements.

4. IT Governance Principles

1. Strategic Alignment: Align IT strategy with organizational goals and business processes.
2. Value Delivery: Ensure that IT delivers the expected benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
3. Risk Management: Recognize the applicability and significance of risks, and ensure they are adequately managed.
4. Resource Management: Use IT resources, including infrastructure, applications, information, and people, responsibly and efficiently.
5. Performance Measurement: Monitor the strategic implementation and delivery of IT services through a set of defined metrics.

5. Information Security Governance Principles

1. Security Policy: Establish a written information security policy that provides direction and support for security in accordance with business requirements and relevant laws and regulations.
2. Organization of Information Security: Maintain a security organization structure with defined roles and responsibilities that does not have any conflict of interest.
3. Asset Management: Identify, classify, and manage IT and information assets.

4. Human Resource Security: Ensure that employees, contractors, and third-party users are aware of and fulfill all their information security responsibilities.
5. Physical and Environmental Security: Secure physical and electronic areas, prevent unauthorized physical access, damage, and interference.
6. Access Control: Limit access to information and IT assets to only those who need access to perform their roles.

6. Standards and Regulations

Vivriti Capital Limited adheres to the following standards and regulations:

1. ISO27001:2022 - Information Security Management System.
2. ISO27701:2019 - Privacy Information Management.
3. Data Protection and Digital Privacy (DPDP) Act - To ensure personal data is handled with respect for privacy and security.
4. COBIT - For developing, implementing, monitoring, and improving IT governance and management practices.

Additionally, Vivriti Capital Limited will strictly adhere to all rules, circulars, and guidelines released by the RBI for NBFCs.

7. Roles and Responsibilities

- Board of Directors: Ensure that IT and Information Security Governance aligns with business needs.
- Chief Technology Officer (CTO): Implement and oversee the IT strategy.
- Head of Information Security (DPO): Ensure the implementation and maintenance of the security policies and practices.
- Tech team: Execute the IT strategy, manage resources, and ensure continuous service delivery.
- All Employees: Comply with all IT and information security policies, procedures, and standards.

8. Review and Amendments

This framework and policy will be reviewed annually or as deemed necessary in the light of any significant changes to the business, regulations, or breaches of security. Any changes made will be communicated to all stakeholders.

9. Conclusion

The IT Governance Framework & Information Security Governance Policy aims to provide a structured approach for effective IT and security management in Vivriti Capital Limited. All stakeholders must adhere to this policy to ensure regulatory compliance, security of assets, and alignment with business objectives.

