Vivriti Capital Limited

Audit Policy

Version 3.0

Project/ Track Name	Vivriti Capital
Document Name	Audit Policy
Document No	ISP-15
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

1 Purpose

- The Audit Program is planned to take into consideration the status and importance of the process and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency, and methods are predefined. Selection of auditors and conduct of audits ensures in achieving objectivity of the audit process.
- Vivriti Capital shall conduct ISMS audits and appropriate follow up to ensure compliance with the Vivriti Capital's ISMS policies, procedures, standards, and guidelines within scope of the ISMS, by devising standard documentation for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.
- Vivriti Capital shall also conduct technical compliance review to evaluate and assess its networks and application and ensure adequate protection from latest vulnerabilities.
- Vivriti Capital shall also conduct internal audits to ensure that the IT processes and technologies implemented are compliant with Vivriti Capital's security policies and standards.
- As a part of this, the accountability and course of activities for corrective actions and preventive actions taken for taking action to eliminate the cause of nonconformities with the ISMS requirements to prevent recurrence are documented in next sections.
- Vivriti Capital will integrate privacy management within the ISMS audits aligning with ISO27701:2019, ensuring both security and privacy concerns are addressed adequately. Compliance with DPDP Act, 2023 and RBI Digital Lending Guidelines will be considered to ensure data protection, privacy and ethical lending practices.

2 Scope

- The document intends to define the framework for conducting periodic internal audit of Information Security Management Systems (ISMS) established at Vivriti Capital. This follows Vivriti Capital Information Security Policy where the management has committed continual monitoring at management level to ensure compliance with the Information Security Policies and Procedures adopted within Vivriti Capital.

3 Objective

- The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.
- The IS Audit will also assess the alignment with DPDP Act,2023, ensuring data protection and privacy are prioritized and embedded in all IT and business processes. Furthermore, adherence to RBI Digital Lending Guidelines will be evaluated to ensure ethical, transparent, and secure digital lending practices

3.1 Modification Guidelines

- The document is owned and maintained by the Head of Information Security and Privacy. Any requests for changes to this document must be provided to Head of Information

Security and will update the document, as appropriate. Until the document is updated, approved, and posted into the Vivriti Capital policies and procedures, the existing process must be followed, unless a deviation request has been granted.

3.2 Exception Request

- It is expected that employees implementing ISMS process will apply their best judgment in every situation to determine the best course of action for Vivriti Capital. This may occasionally require exception from the approved ISMS process. Any exception to this procedure must be requested and documented.

3.3 References

- The guidelines have reference to Information Security Policy of Vivriti Capital, and these documents must be read in conjunction.

4 Ownership and Responsibilities

- Vivriti Capital aims at continually improving the effectiveness of the ISMS using the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review of the Information Security Management System implemented at Vivriti Capital.
- The ISMS internal auditor must monitor the processes being followed by the various teams and must conduct periodic reviews to ensure compliance with Vivriti Capital ISMS policies, procedures, standard, and guidelines.
- A comprehensive internal audit shall be conducted half-yearly with results being reported to Vivriti Capital management for corrective and preventive action.
- Half-yearly Internal Assessment can be conducted by the independent auditor or with the help of Third-Party Vendor.
- Vivriti Capital will consider the principles of privacy, data protection, and ethical digital lending practices in the ISMS. Procedures will be adapted to incorporate guidelines from DPDP Act,2023 and RBI Digital Lending Guidelines, ensuring a holistic approach to information security and privacy.

5 Review

- The procedure would be reviewed every year, else whenever required.
- The procedure will be reviewed bi-annually or whenever required, considering updates or changes in ISO27001, ISO27701, DPDP Act, 2023, and RBI Digital Lending Guidelines to ensure ongoing compliance and effectiveness.

6 Procedure

6.1 Managing an Audit Program

Vivriti Capital grants the authority to the Information Security Committee for managing audit program

for Information Security Policies and Procedures and their implementation in Vivriti Capital with the

intent to:

- Establish the objective and scope of the audit program.
- Establish the responsibilities, resources, and procedures.
- Ensure the implementation of the audit program.
- Monitor, review and improve the audit program; and
- Ensure the appropriate audit program records are maintained.

Objectives of an audit program are based on consideration of:

- Management system requirements.
- Standards requirements.
- To obtain and maintain confidence in the ISMS.
- Confirm to the requirements of the ISO 27001, SOC2 and other relevant legislation and regulations.
- Confirm to the identified information security requirements.
- Confirm effective implementation; and
- Perform as expected.

Extent of audit is determined by:

- Scope, objective and duration of each audit.
- The results of previous audits or a previous audit program review.
- Significant changes in organization or ISMS processes; and
- Compliance status.

6.2 Preparing Audit Plan and Conducting Audits

- Information Security Committee shall prepare a half-yearly plan for ISMS audit, which shall include ISMS controls audit and results of technical testing for Information Systems presently being outsourced to external agency/auditors. The audit plan shall be approved by Vivriti Capital management.
- In the event of any change in the Audit Plan, the Team shall prepare a revised audit plan and communicate the same to steering committee for SOC2 implementation.

- For technical testing of Information Systems, the prior approval of the Asset Owner shall be obtained. Adequate precautions shall be taken before the execution of technical testing.
- The execution of audits may be outsourced to capable third parties and internal audit compliance team. The Team shall provide the auditor with information regarding the areas of focus and the audit report formats.
- Audit tests that could affect system availability shall be run outside business hours.
- Audit requirements for access to systems and data should be agreed with appropriate management.
- Requirements for special or additional processing shall be identified and agreed.
- Audits will consider the specific requirements of DPDP Act, 2023, assessing the organization's compliance with data localization, consent mechanisms, and data subjects' rights.
- Adherence to RBI Digital Lending Guidelines will be evaluated, focusing on the transparency, privacy, and security of digital lending operations.

6.3 Access Controls for Auditors

- Audit tests shall be limited to read-only access to software and data.
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.
- All access shall be monitored and logged to produce a reference trail.
- Auditors shall adhere to the guidelines of data protection and privacy as per the DPDP Act, 2023 ensuring that data confidentiality and privacy are not compromised during the audit.

6.4 Deliverables

The following deliverables may be created as a result of this process:

- Internal Audit Program (Half-yearly Audit Calendar)
- Audit Reports
- Corrective and Preventive Actions (as per the CAPA Procedure)
- Statement of applicability if there are any changes

- Data Protection and Privacy Audit Report (aligned with ISO27701:2019 and DPDP Act,2023)
- Digital Lending Compliance Report (as per RBI Digital Lending Guidelines)

6.5 Measurements

- Compliance status of previous audit report per business function audited:
  - Number of audit observations overdue Vs. Total no of audit observations reported.
  - Number of audit observations closed Vs. Total number of audit observations for business function.
  - Compliance status with DPDP Act, 2023, and RBI Digital Lending Guidelines.
  - Effectiveness of data protection and privacy controls and processes.

6.6 Data Protection and Privacy

- Vivriti Capital will include a data protection and privacy audit aligned with ISO27701:2019 and DPDP Act,2023, ensuring personal data is handled with utmost confidentiality, integrity, and availability.
- Data protection impact assessments will be conducted regularly to identify and mitigate risks to data subjects' privacy.
- Procedures and controls for data processing, storage, and transfer will be reviewed and enhanced to ensure compliance with legal and regulatory requirements.

6.7 Digital Lending Audit

- Vivriti Capital will evaluate its digital lending processes to align with RBI Digital Lending Guidelines ensuring transparency, fairness, privacy, and security in digital lending operations.
- The audit will review the disclosure mechanisms, grievance redressal systems, and data security protocols specific to digital lending.

7 Training and Awareness

- All employees, including the audit team, will be trained and made aware of the requirements and guidelines under ISO27001:2022, ISO27701:2019, DPDP Act, 2023, and RBI Digital Lending Guidelines.
- Specific training modules on data privacy and protection, and ethical digital lending practices will be introduced to ensure understanding and compliance.