SATYA MICROCAPITAL LIMITED

Information System Audit Policy

Version 1.1

November 2025

Information System Audit Policy

Purpose of Information System Audit

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.

Role of Information System Audit

IS Audit shall cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit shall also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

Information System Audit Process

The information System Audit Process has defined the comprehensive approach to fulfill the need of the organisation. The details of audit approach are as follows:

Approach

The purpose of audit approach is to enable the development of a strategic work plan that is designed to best meet the organizations objectives. The approach in summary entails the following key phases:

The audit approach has 5 steps to laying down the strong internal audit foundation. The detail of the above-mentioned graph is as follows:

Audit Plan Development - The audit plan is designed to identify and concentrate on areas of importance, to provide an effective and efficient review and seek to add value to the organization's activities. Detailed plans are prepared and updated annually. In the audit planning it is important to identify the key auditable areas followed by the plan approval and plan review and update.

In performing our Statutory Audit of Financial Statement in accordance with the applicable Standards and laws, we intend to obtain a reasonable assurance on the automated/programmed controls. Our

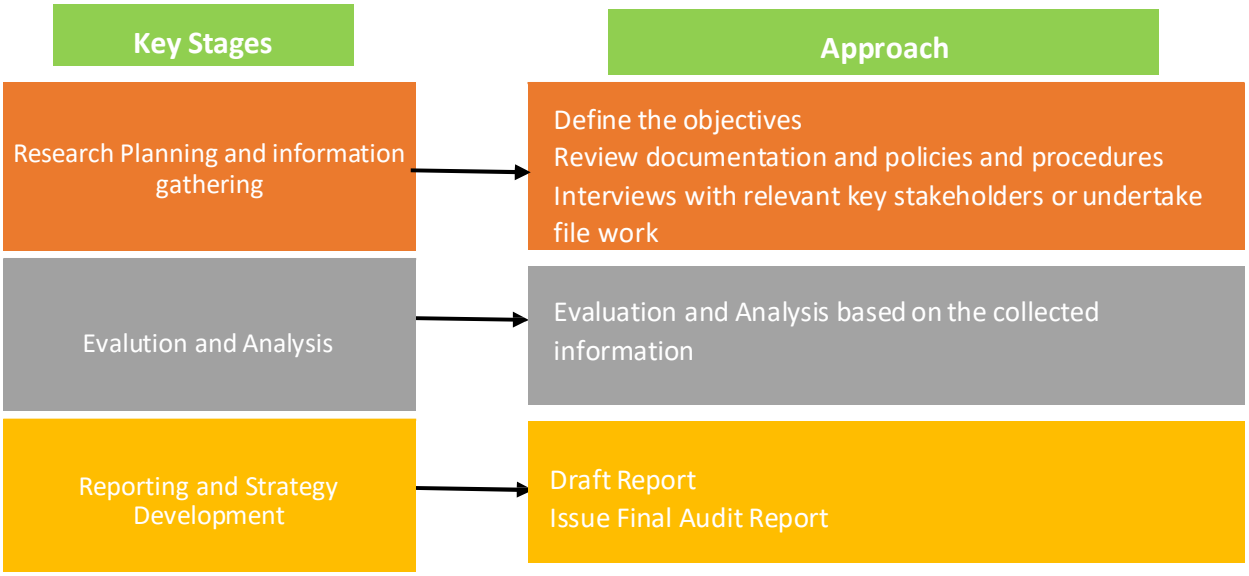
reliance on automated/programmed controls is dependent on effectiveness of IT General Controls. Accordingly, we need to perform a review of IT General Controls.

Therefore, in SATYA following areas has been identified and priorities which shall be audited by the third party on a quarterly basis.

1. Program Development/Change involving
- Test
- Version Control
2. Logical Access Controls for the identified applications involving
- Granting
- Modification
- Deletion
- Password Controls
- Critical id management
- Remote Access Management
- Access Controls over Version Control software (if Version Control software isused)
3. Security Management Process involving
- Hardening of OS and Database
- Infrastructure Change management
4. Computer Operations
- Backup of data and applications
- Job scheduling / monitoring of interfaces
- Incident / problem management
5. Application Controls

Audit Programme Delivery

Specific audits will be undertaken in accordance with the agreed audit plan. The key steps and audit approach in conducting an audit are highlighted below:



Audit Reporting and Documentation

The third-party Audit team will report to SATYA's management which includes MD, Dy CEO, CRO and IT Head) on a quarterly basis on:

- Audits completed
- Progress in implementing Internal Audit work plans
- The status of the implementation of agreed audit recommendations.

Once the audit findings are reviewed by the management. The audit findings are further reported to the IT Strategy Committee.

Active user review by Internal Auditor

The Internal Auditor shall perform quarterly reviews of active users on BR.net against HR records to ensure no unauthorized users exist in the system. This process involves verifying the alignment of user access with current employee status and roles, identifying any discrepancies, and taking corrective actions as necessary. The findings from these reviews shall be documented and reported to the IT Strategy Committee for oversight and further action.IT Strategy Committee

IT Strategy Committee is set up to effective implementation of Cyber Security Policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address

deficiencies and follow-up. The Committee shall meetat least on quarterly basis. The committee shall comprise of

i. Minimum of three directors as members

ii. The Chairperson of the ITSC shall be an independent director and have substantial IT expertise in managing/ guiding information technology initiatives; and

iii. Members are technically competent

iv. CISO shall be the permanent invitee

Following are the Roles and Responsibilities of IT Strategy Committee:

- Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
- Ensuring IT investments represent a balance of risks and benefits, and those budgets are acceptable.
- Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of ITresources.
- Ensuring proper balance of IT investments for sustaining NBFC's growth and becoming aware about exposure towards IT risks and controls.
- Ensuring that Committee should meet atleast on quarterly intervals.
- all other roles and responsibilities as prescribed under Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, November 2023.

Compliance

SATYA management and IT Department is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Also, Internal Audit's performance encompasses the following responsibilities:

- To ensure all work complies with internationally recognized standards
- To maximise use of resources,
- To minimise costs
- To supplement resources where necessary with professional expertise on an as required basis

The company is committed to ensuring adherence to the requirements outlined in the Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices, issued in November 2023.