Sonata Finance Private Limited

# IS audit Policy

Ver 1.0

Classification: *Internal use*

| | |
|---|---|
| Prepared by: | *Megha Goel, Head Planning and Monitoring* |
| Reviewed by | *Anup Singh, MD & CEO Sonata Finance* |
| Approved by | *Anal Jain, Chairman IT Strategy Committee* |

## Version History

| Sl No | Description of change | Version number | Date |
|---|---|---|---|
| 1 | First release | 1.0 | 16th of April 2018 |
| | | | |
| | | | |

## Table of Contents

## Introduction

IS audits are a critical component of ensuring the effective governance of information systems in the organization. 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.

## Purpose:

The purpose of this document is to define an organization wide IS audit policy enabling the effective conduct and management of IS audits and appropriate and timely corrective and preventive actions

## Scope:

The scope of IS audits in SFPL will cover, but not be limited to the following:

1. Effectiveness of IT policies and oversight of IT systems,
2. Adequacy of processes and internal controls for IT and supported business processes.
3. Effectiveness of corrective action to address deficiencies and related follow-up processes.
4. Effectiveness of business continuity plans, and testing of implemented Business continuity plans
5. Status of compliance to all the applicable legal and statutory requirements.

## Policy

1. IS audits shall be conducted at least once in a year.
2. Audits shall be conducted as per a published audit plan.
3. While planning audits, the following are to be considered, as appropriate:
    a. Significance and complexity of the IT activities
    b. Critical activities carried out and supported by IT
    c. The IT infrastructure [hardware, operating system(s), etc., and application software(s)] used,
    d. Nature of changes if any carried out since the previous audit
    e. Complexity of IT applications
    f. IT architecture in the organization
    g. Nature and degree of IT outsourcing
    h. Findings of previous audits
    i. Results of risk assessment (supporting risk based audits)
    j. Availability of audit trails
    k. Availability and implementation of internal controls
4. Auditors should ensure independence during the audits.
5. Audits may be carried out by internal personnel or outsourced to external agencies, or experts may be engaged to carry out audits in specific areas where required.
6. Auditors should review the robustness of the IT environment and consider any weakness or deficiency in the design and operation of IT controls within SFPL.
7. Substantive testing of IT controls may be carried out by the auditor depending on the outcome of the review of the IT controls.
8. Audit procedures shall be suitably documented.
9. Audit findings shall be suitably protected and retained and shall be suitably recoverable.
10. Computer Assisted Audit Tools (CAATs) may be used in critical areas or functions or processes having financial / regulatory / legal implications, as applicable.
11. Audit findings should be reported at the conclusion of the audit.
12. Action on findings should be carried out within a reasonable timeframe and without delay.
13. Actions should include corrective actions depending on the nature of the findings.
14. As part of this IS audit policy, it is envisaged to provide audit-mode access to auditors/ inspecting/ regulatory authorities, where required.
15. Outcome of the IS audit including status of actions taken shall be reported to the relevant level of management and also the Board of Directors through the Audit Committee of the Board or other suitable mechanism.

## Implementation

1. This board approved IS audit policy shall be implemented within the organization by relevant teams.
2. Compliance to this policy and implementation status shall be evaluated at least annually in keeping with assurance requirements indicated above and reported to the board.