# SUNRISE GILTS & SECURITIES PRIVATE LIMITED

# INTERNAL SECURITY AUDIT PLANNER POLICY

(EFFECTIVE DATE: 10/06/2025)

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

| | |
|---|---|
| **Author:** | PRATIK KUMAR MORE |
| **Owner:** | PRATIK KUMAR MORE |
| **Approved by:** | BOARD OF DIRECTORS |
| **Organization:** | SUNRISE GILTS & SECURITIES PRIVATE LIMITED |
| **Version No:** | 1.1 |
| **Approval Date** | 28/05/2025 |
| **Effective Date:** | 10/06/2025 |

## Document Control

**Document Title** **Internal Security Audit Planner**

## Version History

| Version No. | Version Date | Author | Summary of Changes |
|---|---|---|---|
| 1.0 | 13/06/2019 | PRATIK KUMAR MORE | NA |
| 1.1 | 10/06/2025 | PRATIK KUMAR MORE | Review and Approval of BOD |

## Approvals

| Name | Title | ApprovalDate | Version No |
|---|---|---|---|
| PRATIK KUMAR MORE | Internal Security Audit Planner | 13/06/2019 | 1.0 |
| PRATIK KUMAR MORE | Internal Security Audit Planner | 28/05/2025 | 1.1 |

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

# 1.0 INTERNAL AUDIT PLANNER

## 1.1 PURPOSE

To conduct internal cyber security readiness audits to determine whether the controls, processes and procedures of the organization; conform to the requirements of the standards, information security requirements and relevant legislation or regulations.

## 1.2 SCOPE

The scope of this procedure is to audit the effectiveness of the SUNRISE GILTS & SECURITIES PRIVATE LIMITEDIndia Ltd. SEBI Cyber Security Resilience implementation and the continuous improvements of the same.

## 1.3 POLICY STATEMENTS

This document provides procedures for implementing the Internal Audit section of Security Policy for the SUNRISE GILTS & SECURITIES PRIVATE LIMITED. This document can be used to conduct internal audits to determine whether the controls, procedures and security practices conform to the requirements of the security policies, standards, information security requirements and relevant legislation or regulations.

### 1.3.1 AUDIT SCHEDULE

- An internal audit calendar should be created based on fulfilling the following audit requirements:
  - An Internal audit should be conducted for SUNRISE GILTS & SECURITIES PRIVATE LIMITED on a yearly basis.
  - A technical vulnerability assessment of the security preparedness of the facilities should be done on a yearly basis.
- The audit calendar should be created and/or reviewed and approved by the Technology Officer or Head of IT Security.

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

### 1.3.2 AUDIT PLAN

- The Company shall conduct internal audits of its security management system at planned intervals to determine if its control objectives, controls, processes, and procedures are effectively implemented and maintained, and perform as expected.
- Technology Officer shall conduct an assessment of the existing Information Technology security system, in order to establish a baseline for auditing.
- The internal audit plan shall be created based on the following requirements:
    - Importance of processes and areas to be audited (based on a Risk based audit approach)
    - Review of closure of non-conformityfrom previous audits
    - Ensure that auditors shall not audit their own work

### 1.3.3 AUDIT PROCESS

- The auditor would need to review compliance that are applicable to SUNRISE GILTS & SECURITIES PRIVATE LIMITED at the time of the audit.
- The audit calendar should be communicated to the auditee at least one week prior to the proposed date of audit in coordination with the security coordinator.
- The process and people audit will be conducted by means of interviews with the personnel from the department or process being audited; after ensuring that work performed by the personnel is not hindered.
- The technical audit for devices, servers, laptops and desktops would be conducted using vulnerability assessment tools, scripts and/or manual inspection.
- The auditor should check the implementation of the controls implemented in the environment and their effectiveness.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- The auditor should attempt to identify any new risks or improvements that can improve the security of the work environment.
- The auditor should do a sample audit for the effectiveness of the controls' implementation.
- The auditor should take notes and make observations during the audit process.
- The auditor should fill in the following in the Internal Audit Report:
    - Type of Non-Conformance (Major, minor or observation)
    - Relevant Domains and Controls for the Non-Conformance
    - Description of findings
    - Recommendations for conformance
- Then only after consulting with the Technology Officer the auditor should fill the following details in the Audit Report For:
    - Root Cause Analysis of the Non-Conformance
    - Corrective and Preventive Measures
    - Resources assigned to close non-conformity
    - Confirmatory Audit details
    - Update Non-Conformance Tracker and file after closure
- The audit would end with a closing meeting in which the general compliance level will be revealed. The non-conformances detected in the audit will be communicated to the coordinator of the department for correction of the non-conformances
- The Technology Officer should review the recommended action and obtain management approval for the implementation of the control.
- The Technology Officer is responsible for ensuring that the non-conformances are closed by the proposed closure dates. These non-conformances should be reviewed and closed before the next scheduled audit.
- If the implementation of the recommended control is a long-term activity, an implementation plan needs to be created and tracked.

## 1.4 GUIDELINES FOR DETERMINING TYPES OF NON-CONFORMANCE

### 1.4.1 MAJOR NON-CONFORMANCE

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- A major non-conformance occurs when one of the criteria of the standard is not addressed or has not been addressed adequately. Typically, major non-conformances occur when an organization has not addressed all the requirements of a specific element or criterion.
- They also occur when an organization has put a process or procedure in place but has not implemented it or cannot yet demonstrate effective implementation.
- One of the most common major non-conformances is the failure of an organization to complete a full internal audit and/or management review.
- A major non-conformance can also occur if a significant number of minor non-conformances in a given activity.
  - For example, a minor non-conformance in document control may not in itself constitute a significant problem. But if several problems are found with document control, then this points to a larger systemic document control problem and would constitute a major non-conformance.

### 1.4.2 MINOR NON-CONFORMANCE

- A minor non-conformance by itself doesn't indicate a systemic problem. It is typically an isolated or random incident.
  - An example is if the most current version of a document is not available at an operator's station; the updated version exists but a copy of it is not available for the operator's use and the operator is using an outdated procedure.
  - Other examples are a form without a document control number on it or an internal audit with an overdue corrective action request pending.

### 1.4.3 OBSERVATION

- An observation is, no violation of policy, standards, or procedures defined. It is typically identification that there may be a better way to perform an activity.
- The improvements may be in the monitoring of a process or in the documenting of a procedure. Observations are a potential for improvement - a way to avoid future problems.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD