SISL-IT-POL-IT Governance and Audit Policy

Version No: V 1.0

INTERNAL DOCUMENT

OCTOBER 2025

Document Control

Document Name	SISL-IT-POL-IT Governance and Audit Policy
Abstract	This document describes IT Governance and audit at Share India Group
Security Classification	Internal
Location	Share India Group– Delhi

Authorization		
Document Owner	Reviewed by	Authorized by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	**Modification Date DD MMM YYYY**	**Section**	**A/M/D**	**Brief description of change**
1.0	30th October 2025	Initial Version	A	Final

Distribution list
Designated Officer (DO)
Information Security Steering Committee (ISSC)
ISMS Core Team
Auditors (Internal & External)
All users at Share India Group

Table of Content

1 Introduction

SISL is committed to maintaining a robust framework that ensures accountability, transparency, and effective management of IT risks. Regular internal and external audits are conducted to assess compliance with CSCRF, information security standards, and regulatory obligations. All stakeholders including management, IT teams, and third-party service providers are required to adhere to this policy to maintain the confidentiality, integrity, and availability of SISL's information assets.

2 Policy Statement

This policy establishes a comprehensive framework for strategic oversight, effective risk management, and adherence to all applicable regulatory and industry standards, including SEBI's Cybersecurity and Cyber Resilience Framework (CSCRF), ISO 27001, and the DPDP Act. This policy defines a robust governance structure, clear roles and responsibilities, and periodic audit mechanisms designed to ensure that all IT assets, processes, and services are managed securely, efficiently, and in alignment with SISL's business objectives and long-term strategic vision.

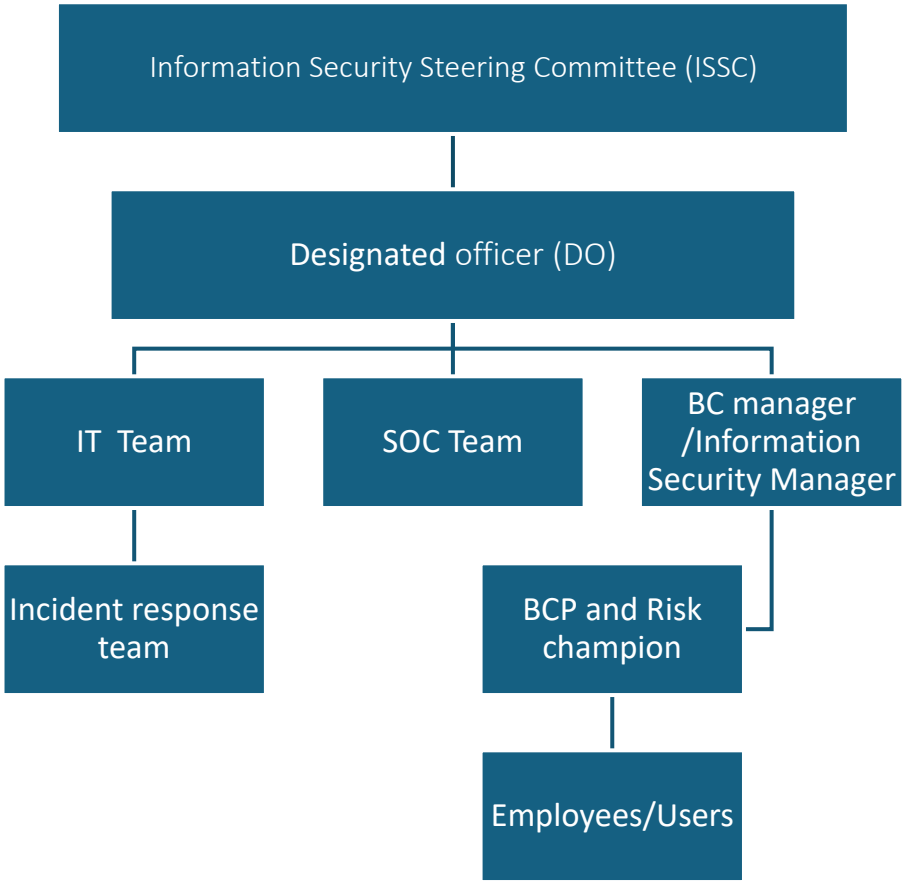
The policy emphasizes proactive identification and mitigation of risks, continuous improvement of IT and cybersecurity practices, and accountability through regular internal and external audits. By integrating governance with operational and technical controls, SISL ensures the confidentiality, integrity, and availability (CIA) of critical information assets, while fostering a culture of compliance, transparency, and operational excellence across the organization.

3 Scope

This policy applies to:

- All SISL information systems.
- All employees of SISL.
- All SISL owned Desktops/ Laptops / Mobile used by the employees of SISL
- All third Party personnel/ contractors who work on SISL's premises or who remotely connect from their network to SISL's network

4 Governance framework



4.1 Description of CSCRF Governance Structure

4.1.1 Board of Directors / ISSC & Crisis Management Team

- Provides top-level cybersecurity and risk oversight.
- Approves Information Security, BCP, and IT Governance policies.
- Reviews critical risks, incidents, and audit findings.
- Oversees cybersecurity posture, risk registers, and BCP readiness.
- Meets at least twice a year (as per CSCRF).
- Activate Crisis Management Plan (CMP) during severe incidents impacting business continuity.
- Conduct a thorough post-crisis analysis to evaluate the effectiveness of response measures, communication strategies, and decision-making during the incident.
- Identify root causes and systemic gaps that contributed to the crisis or delayed response.

- Document lessons learned and prepare a detailed post-incident report and communicate key takeaways to the Information Security Steering Committee (ISSC) and management for future readiness.

4.1.2 Designated Officer (DO)

The DO (Designated officer) is a senior-level executive responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats. DO is the nodal officer to interact with NCIIPC for feedback, trainings, advisories, breach reporting etc. A DO is typically a skilled leader and manager with a strong understanding of information technology and security, who can communicate complicated security concepts to both technical and nontechnical employees.

To effectively perform his/her duties, DO should possess the following:

- Management capabilities like reporting high-risk findings to ISSC and Board.
- Strategic planning abilities
- Knowledge of relevant legislative or regulatory requirements such as IT Act and associated Rules
- Some competence/exposure in the field of information security
- Good communication and writing skills.
- Own CSCRF implementation and security governance.
- Coordination with IT, SOC, BC Manager, ISM, and Risk Champions.

4.1.3 IT Team

- Perform configuration management of all IT systems and network components.
- Ensure timely patch management for servers, endpoints, and applications.
- Maintain and update the IT Asset Inventory and ensure asset classification.
- Support backup and restoration activities in coordination with BCP Team.
- Assist SOC and DO in addressing technical vulnerabilities identified during VAPT or audits.
- Implement secure configurations and hardening standards for OS, databases, and network devices.

4.1.4 SOC Team

- Provide 24x7 monitoring of security events, logs, and network traffic.

- Analyze alerts from SIEM/EDR solutions and correlate with threat intelligence.
- Detect, investigate, and escalate potential security incidents in real time.
- Conduct continuous vulnerability scanning and anomaly detection.
- Maintain and fine-tune monitoring rules, dashboards, and incident triggers.
- Prepare daily, weekly, and monthly security reports for DO and ISSC.

4.1.5 Incident Response Team

- Respond to security incidents, cyber attacks, and critical system failures.
- Coordinate with IT and SOC teams to contain, mitigate, and recover from incidents.
- Ensure communication with SEBI/CERT-In for regulatory incident reporting.
- Lead root cause analysis (RCA) and post-incident reviews to avoid recurrence.

4.1.6 Business Continuity (BC) Manager

- Leads BCP and ITDR planning, testing, and reporting.
- Coordinates with Risk Champions and ISMs to assess BCP readiness.
- Ensures restoration timelines (RTO/RPO) are validated.

4.1.7 Information Security Manager (ISM)

- Implements information security controls at department/BU level.
- Works under DO to enforce access control, data classification, and policy compliance.
- Ensures that periodic activities pertaining to information security are getting carried out without any discrepancies.
- Conducts periodic risk assessments and reports deviations.

4.1.8 BCP and Risk Champions

- Embedded within departments to identify, track, and escalate risks.

- Work with ISM and BC Manager to update the Risk Register
- Includes IT, operations, and critical business process owners.
- Responsible for conducting BCP drills and ensuring recovery measures are operational.

4.1.9 All Employees

- Acceptable usage, awareness, and reporting of threats.

SISL shall ensure that all individuals involved in IT governance, cybersecurity, and audit functions including members of the Information Security Steering Committee (ISSC), Risk Champions, Business Continuity Managers, and Information Security Managers are adequately trained on their governance roles and responsibilities.

Regular awareness sessions and workshops shall be conducted on:

- CSCRF control domains and governance expectations
- Roles defined in the governance framework
- Regulatory obligations (e.g., SEBI, DPDP, ISO 27001)
- Audit lifecycle and post-audit responsibilities

Participation in such training shall be documented and reviewed annually by the DO and reported to the ISSC.

5 Audit Framework

5.1 Audit Types and Frequencies

Audit Type	Scope	Frequency	Auditor Requirements
Internal ISMS Audit	Covers CSCRF domains including IT processes, access control, patch management, and SOC etc.	Half Yearly	Conducted by internal InfoSec team and reports reviewed by DO & ISSC
External IT Audit	Comprehensive CSCRF controls verification	Annual	Independent external auditor (CERT-In empanelled or SEBI-approved)
Regulatory / SEBI Cyber Audit	Compliance with SEBI's circulars and CSCRF mandates	As per SEBI mandate (annual)	Conducted by SEBI-approved auditors

5.2 Audit Methodology

5.2.1 Audit Planning

- Prepare an Annual Audit Plan/Calendar covering internal audits, external audits, VAPT, and regulatory audits.
- Define the scope, objectives, and criteria of each audit (e.g., CSCRF domains – ID, PR, DE, RS, RC).
- Assign auditors (internal/external) ensuring independence from day-to-day IT operations.
- Identify evidence sources (e.g., policies, logs, configurations, incident reports).

5.2.2 Risk-Based Audit Approach

- Prioritize audits for critical assets, high-risk processes, and regulatory requirements.
- Use risk ratings (Critical, High, Moderate, Low, Very Low) to classify findings.
- Conduct technical testing (VAPT, config review) alongside process checks (policy compliance, access controls).

5.2.3 Execution

- Conduct interviews, document reviews, log analysis, and technical tests.
- Collect evidence and validate compliance with CSCRF controls.
- Record non-conformities, gaps, or improvement opportunities.
- Verify compliance with ISO 27001 Annex A controls where applicable.

5.3 Audit Reporting

5.3.1 Draft Report Preparation

Prepare a draft audit report summarizing:

- Scope and Objectives
- Audit Findings (Critical/High/Moderate/Low)
- Root Cause Analysis
- Impact Assessment
- Recommended Corrective Actions

5.3.2 Management Review

- Review draft report with DO, ISM, IT Team, and Risk Owners for validation.

- Finalize the report with a Corrective and Preventive Action Plan (CAPA).

5.3.3 Submission

- Internal Audit Reports: Shared with ISSC on a quarterly basis.
- External Audit Reports: Submitted to Board of Directors and, where required, SEBI/CERT-In.
- Maintain audit records as evidence for regulatory reviews.

5.4 Audit Closure

5.4.1 Corrective Action Tracking

Track each finding in an Audit Action Tracker (Excel) with:

- Assigned Owner
- Risk Rating
- Target Closure Date
- Status (Open/In Progress/Closed)

5.4.2 Closure Verification

- ISM and Internal Audit team verify remediation actions (evidence-based).
- Critical/High findings must be resolved within 30 days (as per CSCRF expectations).

5.4.3 Post-Audit Review

- Conduct a post-audit review to evaluate process improvements.
- Update policies, SOPs, and configurations to avoid repeat findings.

5.4.4 ISSC Oversight

- ISSC reviews closure status in quarterly governance meetings.
- Unresolved risks or critical findings are escalated to Board and Management.

6 Policy Review Frequency

The policy shall be reviewed annually or when there is a major change within Share India Securities Limited environment.

7 Policy Exception

In case of any deviation against policy guidelines, Risk Acceptance form should be submitted to Designated Officer for approval.

8 Policy Violation Reporting Matrix

Any violation to the policy should be reported to Reporting Manager/Designated Officer

Level	Designation
Level 1	Employee's Reporting Manager
Level 2	Designated Officer
Level 3	MD & CEO