

PRO-07: ISMS INTERNAL AUDIT PROCEDURE

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | Doc ID: JT-ISMS-PRO-007

Version: 1.0 | Effective Date: 14-Oct-2026 | Review Cycle: Annual

ISO/IEC 27001:2022 Clause Mapping: Clause 9.2 (Internal Audit)

1. Purpose & Scope

This procedure establishes the process for planning, conducting, reporting, and tracking internal audits of the Information Security Management System (ISMS) to ensure compliance with ISO/IEC 27001:2022, organizational security policies, and legal requirements.

2. Auditor Qualifications & Independence (Clause 9.2)

- Auditor Competence:** Internal auditors must be trained in ISO/IEC 27001:2022 standard requirements and audit techniques.
- Objectivity & Impartiality:** Auditors shall not audit their own work, departments, or direct deliverables (e.g., a DevOps engineer cannot audit cloud infrastructure security).

3. Annual Internal Audit Program Cadence

- The ISMS must undergo a full-scope internal audit at least **once per calendar year** or prior to any major external certification/surveillance audit.
- The audit program encompasses:
 - Mandatory Clauses 4 through 10 of ISO/IEC 27001:2022.
 - All 93 controls of ISO/IEC 27001:2022 Annex A detailed in the Statement of Applicability (REG-02).

4. Internal Audit Process Flow

- Audit Planning:** Lead Auditor issues the Audit Plan at least 10 business days before audit commencement, specifying scope, dates, and auditees.
- Execution:** Auditors conduct interviews, examine documented evidence, sample access configurations, inspect CI/CD pipelines, and review logs using CHK-01.
- Categorization of Findings:**

- **Major Nonconformity (Major NC):** Complete absence or systemic breakdown of a required clause or control; significant risk of data breach.
 - **Minor Nonconformity (Minor NC):** Isolated lapse or inconsistency with no direct security compromise.
 - **Opportunity for Improvement (OFI):** Suggestion to optimize security practices.
1. **Audit Reporting:** Lead Auditor publishes the Internal Audit Report within 5 business days of the closing meeting.
 2. **Corrective Action Tracking:** All Major and Minor NCs must be logged into the Corrective Action Register (REG-05) and resolved per PR0-09 .