

# PRO-08: ISMS MANAGEMENT REVIEW PROCEDURE

## JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | Doc ID: JT-ISMS-PRO-008

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

ISO/IEC 27001:2022 Clause Mapping: Clause 9.3 (Management Review)

### 1. Purpose & Frequency

To ensure top management's continuing suitability, adequacy, and effectiveness of the ISMS, the Board of Directors conducts a formal Management Review Meeting (MRM) at least **annually** (or semi-annually during initial certification).

### 2. Mandatory Input Agenda Items (Clause 9.3.2)

The review must formally evaluate:

- Status of actions from previous management reviews.
- Changes in external and internal issues relevant to the ISMS (legal, regulatory, technology changes).
- Changes in needs and expectations of interested parties (clients, RBI, CERT-In, DPDP Act).
- Feedback on information security performance, including:
  - Nonconformities and corrective actions status ( REG-05 ).
  - Monitoring and measurement results against security objectives ( D0C-03 ).
  - Internal and external audit results.
- Feedback from interested parties (customer audits, security inquiries).
- Results of the annual risk assessment and status of the Risk Treatment Plan ( REG-01 ).
- Opportunities for continual improvement.

### 3. Mandatory Review Outputs (Clause 9.3.3)

Decisions and actions documented in the formal meeting minutes ( TEM-01 ) must address:

- Opportunities for continual improvement of the ISMS.
- Any necessary changes to the scope, policies, or objectives of the ISMS.
- Resource allocations (budget, staffing, software tooling) required for security.

## 4. Documentation & Sign-off

---

Minutes of the Management Review must be signed by the Managing Director and retained as official documented information for at least 3 years.