

DOC-03: ISMS OBJECTIVES, METRICS & MEASUREMENT PROGRAM

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | **Doc ID:** JT-ISMS-DOC-003

Version: 1.0 | **Effective Date:** 14-Oct-2026

ISO/IEC 27001:2022 Clause Mapping: Clause 6.2 (Information security objectives and planning to achieve them), Clause 9.1 (Monitoring, measurement, analysis and evaluation)

1. Purpose

In accordance with ISO/IEC 27001:2022 Clause 6.2 and Clause 9.1, JOHN THOMAS FINTECH PRIVATE LIMITED establishes quantifiable, measurable, and strategically aligned Information Security Objectives to evaluate the effectiveness and maturity of our ISMS.

2. Core Security Objectives & KPI Dashboard

Ref #	Objective Statement	Target KPI	Measurement Metric	Frequency	Owner
OBJ-01	Ensure continuous availability and resilience of fintech transaction systems	≥ 99.95% Availability	$\frac{(\text{Total Minutes} - \text{Downtime Minutes})}{\text{Total Minutes}} \times 100$	Monthly	DevOps Lead
OBJ-02	Rapid remediation of critical & high infrastructure/application vulnerabilities	Critical: 100% within 48h High: 100% within 7d	Elapsed hours from CVE detection to verified production deployment	Monthly	Engg Lead & DevOps
OBJ-03	Ensure organizational security awareness and cyber vigilance	100% completion	% of workforce passing annual security training & phishing assessment	Quarterly	CISO / HR
OBJ-04	Prevent unauthorized data breaches and customer PII compromise	Zero (0) incidents	Number of confirmed data breaches or unauthorized data leaks	Continuous	CISO
OBJ-05	Prompt detection and containment of security incidents	P1: < 60 min containment CERT-In: < 6h report	Time from detection to containment; CERT-In notice timestamp	Per Incident	CISO / Incident Lead
OBJ-06	Maintain rigorous backup integrity and data recoverability	RPO < 15 min RTO < 4 hours	Biannual disaster recovery restoration drill success rate	Bi-annually	DevOps Lead
OBJ-07	Strict enforcement of multi-factor authentication and identity security	100% MFA compliance	% of cloud/admin accounts	Monthly	IT / DevOps

			with MFA enforced		
OBJ-08	Vendor security risk assurance across critical fintech suppliers	100% Tier-1 suppliers assessed	Number of active critical suppliers with current security assessments	Annually	CISO
OBJ-09	Effective resolution of internal and external audit findings	100% within agreed SLA	% of Corrective Action Requests (CAR) closed within target due date	Bi-annually	CISO

3. Evaluation & Reporting Mechanism (Clause 9.1)

- 1. Monthly Security Dashboard:** CISO compiles technical metrics (uptime, vulnerabilities, patching SLAs, access audits) into the Monthly Information Security Metric Report.
- 2. Quarterly ISC Review:** Information Security Committee evaluates trends, repeats, or failing metrics and issues corrective directives.
- 3. Annual Management Review:** Top Management formally reviews performance against these objectives during the Management Review Meeting (TEM-01). Objectives failing to achieve targets require mandatory Corrective Action (PR0-09).

4. Document Control & Approvals

Version	Date	Author	Approver
1.0	14-Oct-2026	CISO / Security Lead	John Thomas, Managing Director