

DOC-02: ISMS ROLES, RESPONSIBILITIES & RACI MATRIX

JOHN THOMAS FINTECH PRIVATE LIMITED

CIN: U62099KL2026PTC106017 | Doc ID: JT-ISMS-DOC-002

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

ISO/IEC 27001:2022 Clause Mapping: Clause 5.3 (Organizational roles, responsibilities and authorities), Control 5.2 (Information security roles and responsibilities), Control 5.3 (Segregation of duties)

1. Purpose & Organizational Structure

To ensure unambiguous accountability for information security across JOHN THOMAS FINTECH PRIVATE LIMITED, this document defines the governance hierarchy, specific security roles, and an operational RACI matrix covering all ISO/IEC 27001:2022 domains.



2. Roles and Key Responsibilities

2.1 Board of Directors (Top Management)

- **Members:** John Thomas (Managing Director), Saramma Thankachen (Director).
- **Responsibilities:**
 - Authorize and sign the overarching Information Security Policy (P0L-01).
 - Allocate necessary annual financial budget, human resources, and tooling for security.
 - Review ISMS performance and audit outcomes during the bi-annual Management Review Meeting (MRM).
 - Provide strategic direction and enforce organizational compliance.

2.2 Information Security Committee (ISC)

- **Composition:** Managing Director, CISO / Security Lead, Engineering Lead, and Legal/Compliance Advisor.
- **Responsibilities:**
 - Meet quarterly to review security posture, emerging threats, and audit findings.
 - Evaluate risk assessment results and approve the Risk Treatment Plan (REG-01).
 - Oversee significant technology changes, new fintech platform rollouts, and major vendor approvals.

2.3 Chief Information Security Officer (CISO) / Security Lead

- **Responsibilities:**
 - Day-to-day governance of the ISMS and adherence to ISO/IEC 27001:2022.
 - Maintain the Statement of Applicability (REG-02) and Risk Register (REG-01).
 - Coordinate internal security audits, external certification audits, and vulnerability assessments (VAPT).
 - Serve as the primary liaison for statutory regulatory filings with CERT-In and Data Protection Board under DPDP Act 2023.
 - Lead the Security Incident Response Team (SIRT).

2.4 Engineering Lead / Lead Systems Architect

- **Responsibilities:**
 - Enforce Secure Software Development Lifecycle (SSDLC) practices (P0L-09).
 - Implement automated code reviews, SAST, DAST, and container vulnerability scanning.
 - Ensure strict logical segregation of Development, Staging, and Production environments.
 - Manage pull request approval workflows and production deployment gating.

2.5 Cloud Infrastructure / DevOps Lead

- **Responsibilities:**
 - Maintain AWS/GCP cloud security configurations, VPC peering, firewall rules, and security groups.
 - Enforce Multi-Factor Authentication (MFA), role-based access control (RBAC), and least-privilege policies.

- Oversee automated immutable cloud backups, backup restoration drills, and Disaster Recovery procedures (PR0-03).
- Monitor centralized audit logs, CloudTrail, SIEM alerts, and system uptime.

2.6 All Employees & Contractors

- **Responsibilities:**
- Comply with the Acceptable Use Policy (P0L-07) and Clean Desk/Screen Policy (P0L-11).
- Complete mandatory annual security awareness training.
- Protect assigned credentials, encryption keys, and hardware assets.
- Immediately report observed or suspected security incidents, vulnerabilities, or phishing attempts.

3. Segregation of Duties (Control 5.3)

To prevent accidental errors, unauthorized transactions, or undetected malicious modifications:

1. **Dev vs. Prod Segregation:** Software engineers who author code do not hold direct write or administrative access to the live production database or production hosting environment.
2. **Deployment Gatekeeping:** Code merges into production require automated CI/CD pipeline tests, static security scanning pass, and manual peer approval by designated Tech Leads.
3. **Financial / Transactional System Controls:** Access to payment gateway keys, cryptographic signing keys, and bank integration credentials requires multi-party approval.
4. **Audit Independence:** Internal audits (PR0-07) are performed by qualified internal or independent external auditors who do not audit their own operational work.

4. ISMS RACI Matrix

*Legend: **R** = Responsible (does the work), **A** = Accountable (final approval/ownership), **C** = Consulted (provides input), **I** = Informed (notified of status)*

ISMS Process / Deliverable	Top Mgmt	CISO / Sec Lead	Engg Lead	DevOps Lead	Employees
Information Security Policy Approval	A	R	C	C	I
Risk Assessment & Methodology Execution	A	R	C	C	I
Statement of Applicability (SoA) Maintenance	A	R	C	C	I
Access Provisioning & Deprovisioning	I	A	C	R	I
Secure Code Review & Static Analysis (SAST)	I	C	A/R	C	I
Production Cloud Infrastructure Hardening	I	A	C	R	I
Security Patching & Vulnerability Remediation	I	A	R	R	I
Security Incident Response & CERT-In Notice	A	R	C	C	I
Disaster Recovery Testing & Backup Restoration	I	A	C	R	I
Supplier / Cloud Vendor Risk Assessments	A	R	C	C	I
Employee Security Training & Awareness	A	R	I	I	R
Internal Audit Execution & Reporting	A	R	C	C	I
Management Review Meetings (MRM)	A/R	R	C	C	I

5. Document Control & Approvals

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

