Proposal: Foundational Information Security Governance Model

Prepared by: Rameen Mughal
Date: November 03, 2025

Executive Summary

To protect our customers, our company, and our ability to operate, we must establish a formal but reasonable Information Security (InfoSec) program. Our objective is to establish a lightweight yet structured governance model that embeds security into our culture from the outset. This will be achieved by defining clear responsibilities, establishing key security processes, and ensuring accountability through regular reviews and reporting. The ultimate goals are to reliably meet our regulatory obligations and build a foundation of trust with our customers and partners.

Roles and Responsibilities

Roles	Responsibilities
Chief Information Security Officer (CISO)	• Develops and leads the overall Information Security strategy. • Defines policies, standards, and frameworks. • Reports security posture to senior management/board. • Approves risk treatment plans.
IT Team	• Implements technical security controls (firewalls, encryption, backups, etc.). • Manages patching, system hardening, and access control. • Monitors systems for vulnerabilities and incidents.
Risk & Compliance Team (or designated person)	• Maintains the Risk Register. • Performs periodic risk assessments. • Tracks mitigation actions and ensures alignment with regulations (e.g., PCI-DSS, GDPR).
Department Heads	• Ensure employees follow security policies and report incidents.
Employees	• Follow InfoSec policies. • Complete mandatory awareness and phishing training. • Report suspicious activities or incidents immediately.

For a small fintech, security is often a function of the IT team, with the potential to evolve into a dedicated Security team during expansion.

Key Documents & Processes

Document/Process	Purpose
Information Security Policy	Defines the organization's security principles, roles, and acceptable use.
Access Control Policy	Specifies user access management, least privilege, and MFA requirements.
Incident Response Plan	Outlines procedures for detecting, reporting, and managing security incidents.
Risk Register	Tracks identified risks, impact, mitigation, and owner.
Vendor Security Checklist	Ensures third-party services meet security standards.
Training & Awareness Program	Ensures all employees understand security responsibilities.
Compliance Monitoring Report	Documents adherence to laws, standards (ISO 27001, etc.).

Accountability & Compliance Mechanisms

- **Governance Meetings:** Monthly or quarterly InfoSec meetings chaired by the CISO to review risks, incidents, and compliance status.
- **Risk Ownership:** Each risk in the register has a clearly assigned owner responsible for mitigation and reporting progress.
- **Policy Acknowledgment:** Employees must sign acknowledgment forms or confirm electronically that they understand and agree to follow InfoSec policies.
- **Internal Audits & Reporting:** Conduct periodic internal reviews (even lightweight ones) to verify compliance with security policies and controls.
- **Metrics and KPIs:** Track and report key indicators such as:
    - Number of incidents reported
    - % of employees completing training
    - % of systems with latest patches
    - Number of high-risk findings and their status (open/close)
- **Disciplinary Procedures:** Define clear consequences for non-compliance or repeated negligence.

Implementation Roadmap (3-Phase Plan)

Phase 1 – Foundation:

- Appoint a CISO or InfoSec Lead.
- Draft basic policies (Information Security, Access Control, Incident Response).
- Create initial Risk Register.

Phase 2 – Integration:

- Conduct first risk assessment.
- Implement awareness training.
- Establish reporting and escalation processes.

Phase 3 – Maturity:

- Conduct internal compliance reviews.
- Automate logging and monitoring.
- Introduce formal metrics and improvement cycles.

Conclusion

In summary, this governance model provides a simple yet effective framework for managing information security within the startup. By clearly defining roles, responsibilities, and essential processes, it ensures that security is integrated into daily operations rather than treated as an afterthought.

Given the startup's small size, the IT team will also act as the Security Team under the guidance of the CISO, ensuring that technical and security measures are implemented efficiently. Over time, as the company grows, the governance structure can mature to include a dedicated security function and more formalized compliance activities.