Development and Implementation of ISO 27001-Aligned InfoSec Policies

As the newly appointed Information Security Officer at a recently established financial institution, I stepped into a critical role with significant responsibility. The organization currently lacks a formalized set of information security policies, making my expertise vital to laying the foundation for a secure and compliant operating environment.

My primary objective was to develop and implement a comprehensive set of information security policies that align with ISO/IEC 27001 standards. These policies will serve as the cornerstone of the institution's security posture.

1. Review the Current Organizational Structure and Processes

Objective: Understand the organization's operational model to tailor security policies appropriately.

Steps:

- Meet with department heads (IT, HR, Legal, Finance, etc.).
- Map business processes, data flows, and system dependencies.
- Identify critical assets, compliance obligations (e.g., PCI DSS, SOX), and third-party relationships.

2. Identify Key Information Security Policy Requirements (ISO 27001)

ISO 27001 clause 5-10 and Annex A outline the required policy domains

Mandatory core policies

- Information Security Policy (clause 5.2)
- Risk Assessment and treatment policy
- Statement of Application

Annex A Supporting policies

- A.5 Information security roles and responsibilities
- A.6 Mobile device and teleworking policy

- A.9 Access Control Policy
- A.10 Cryptographic Policy
- A.12 Operational security policy
- A.13 Communications security policy
- A.16 Incident management policy
- A.18 Compliance policy

3. Develop Core Policies

Here's a streamlined policy set for a new financial institution, aligned with ISO 27001:

Access Control Policy

- Role-based access (RBAC), principle of least privilege.
- Strong password and MFA requirements.
- Termination process to revoke access promptly.

Data Classification & Handling Policy

- Classify data (e.g., Public, Internal, Confidential, Restricted).
- Define rules for storage, transmission, and destruction.
- Encrypt sensitive data at rest and in transit.

Incident Response Policy

- Define incident types and reporting thresholds.
- Assign response roles (Incident Response Team - IRT).
- Include notification timelines and root cause analysis.

Acceptable Use Policy (AUP)

- Define acceptable behaviors and prohibited actions.
- Cover devices, internet usage, and email practices.

Third-Party Risk Management Policy

- Due diligence checks for vendors.
- Contractual obligations for data protection.
- Ongoing monitoring and audit rights.

Each policy includes:

- Purpose & scope

- Roles & responsibilities
- Key definitions
- Policy requirements
- Non-compliance consequences

4. Align Policies with ISO 27001 and Organizational Context

Ensure:

- Policies reflect actual risk appetite and regulatory needs.
- They support the information Security Management System (ISMS)
- Integration with legal, compliance and IT teams for feasibility

Validation:

- Conduct stakeholder reviews
- Pilot testing in departments
- Incorporate feedback loops for continuous improvement

5. Launch an Awareness & Training Program

Information Security Awareness Program

Components:

- Kickoff training: Introduction to policies and why they matter.
- Monthly topics: Phishing, social engineering, secure remote work, etc.
- Microlearning & quizzes: Reinforce key points in short modules.
- Simulated phishing: Test real-world readiness.
- Policy sign-off: Require acknowledgment from all staff.

Delivery Methods:

- LMS platform
- Email campaigns
- Posters and internal newsletters

Final Deliverables Summary:

- Comprehensive set of InfoSec policies (ISO 27001-aligned)
- Stakeholder-approved policy documentation
- ISMS alignment matrix (mapping ISO controls to policies)
- Awareness & training plan with rollout schedule