# ISO 27001 Compliant Organizational Structure Template

## Introduction:

This document outlines the governance structure required to establish, implement, and maintain an ISO 27001-compliant Information Security Management System (ISMS) for [COMPANY NAME]. The structure ensures clarity in roles, responsibilities, and authority for managing information security.

---

## 1. Organizational Chart

Below is a graphical representation of the ISO 27001-compliant organizational structure. This chart illustrates the hierarchy and reporting lines for effective governance of the ISMS:

Graphical Organization Chart:

- Chief Executive Officer (CEO)  
 - Reports to: Board of Directors  
 - Direct Reports:  
 - Chief Information Security Officer (CISO)  
 - Leads the ISMS implementation.  
 - Coordinates with:  
 - Information Security Committee (ISC)  
 - Information Security Manager (ISM)  
 - Manages:  
 - Departmental Information Security Officers (DISOs)  
 - IT Operations Team  
 - Legal and Compliance Officer  
 - Ensures regulatory compliance.

## 2. Description of Roles and Responsibilities

### Chief Executive Officer (CEO)

- Overall accountability for the ISMS.

- Ensures alignment of ISMS objectives with organizational goals.

- Provides necessary resources and support for ISMS implementation.

### Chief Information Security Officer (CISO)

- Develops and oversees the ISMS.

- Reports ISMS performance to top management.

- Ensures compliance with ISO 27001 requirements and other regulatory obligations.

### Information Security Committee (ISC)

- Composed of representatives from key departments (e.g., IT, HR, Legal, Operations).

- Advises on information security strategies and initiatives.

- Reviews and approves information security policies and procedures.

### Information Security Manager (ISM)

- Coordinates ISMS implementation across departments.

- Conducts risk assessments and manages risk treatment plans.

- Facilitates internal audits and management reviews.

### Departmental Information Security Officers (DISOs)

- Ensure departmental compliance with ISMS policies.

- Act as the liaison between the department and the ISM.

- Conduct departmental security awareness training.

### IT Operations Team

- Implements and manages technical security controls.

- Ensures secure configuration and maintenance of IT infrastructure.

- Monitors for and responds to security incidents.

### Employees and Contractors

- Adhere to [COMPANY NAME]’s information security policies and procedures.

- Report security incidents promptly.

- Participate in mandatory information security training.

## 3. Narrative Context

The organizational structure for [COMPANY NAME] has been designed to promote accountability and ensure effective communication across all levels. The Information Security Committee plays a pivotal role in bridging strategic goals with operational execution. Each role’s responsibilities are clearly defined to foster a culture of continuous improvement and alignment with ISO 27001 requirements.

Regular management reviews, internal audits, and staff training sessions are integral to the ISMS. This governance model ensures that information security risks are effectively managed, supporting [COMPANY NAME]’s commitment to safeguarding sensitive data.

## 4. Revision and Maintenance

This document will be reviewed annually or whenever significant organizational changes occur. Updates will be made to reflect the evolving business and regulatory landscape.

## Approval:

| Name | Title | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |

---