

# Introduction to Security Compliance and Governance

Introduction to Security Compliance & Governance  
(A concise, easy-to-read reference guide)

## 1. Core Concepts

| Term                | Definition                                                                                                                      | Why It Matters                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Security Compliance | Adherence to external laws, regulations, standards, and contractual obligations that dictate how information must be protected. | Avoids legal penalties, protects reputation, and ensures trustworthy operations.                         |
| Governance          | The set of policies, processes, and organizational structures that direct and control security activities.                      | Aligns security with business objectives, clarifies responsibilities, and drives continuous improvement. |
| Risk Management     | Identification, assessment, and mitigation of threats to assets.                                                                | Provides the basis for both compliance (what must be protected) and governance (how to protect it).      |

## 2. Why Organizations Need Both

- Regulatory Pressure** – GDPR, HIPAA, PCI-DSS, CCPA, etc. demand demonstrable compliance.
- Business Drivers** – Customer trust, market differentiation, and investor confidence.
- Operational Efficiency** – Governance creates repeatable processes; compliance checks confirm they work.
- Incident Response** – Clear governance roles speed up detection, containment, and reporting required by compliance frameworks.

## 3. Key Compliance Frameworks (Snapshot)

| Framework | Scope | Primary Audience | Typical Controls |
|-----------|-------|------------------|------------------|
|-----------|-------|------------------|------------------|

# Introduction to Security Compliance and Governance

|                      |                                                                                                        |                                                         |                                                         |
|----------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------|
| <b>GDPR (EU)</b>     | Personal data of EU residents                                                                          | All organizations handling personal data                | Data minimization, consent, breach notification (72?h)  |
| <b>HIPAA (US)</b>    | Protected Health Information (PHI)                                                                     | Healthcare providers, insurers, business associates     | Access controls, audit logs, encryption, risk analysis  |
| <b>PCI?DSS</b>       | Cardholder data                                                                                        | Merchants, payment processors                           | Network segmentation, vulnerability scanning, MFA       |
| <b>ISO/IEC 27001</b> | Information Security Management System (ISMS)                                                          | Any organization seeking a certifiable security program | Risk assessment, asset inventory, continual improvement |
| <b>SOC 2</b>         | Service?organization controls (security, availability, processing integrity, confidentiality, privacy) | Cloud service providers, SaaS                           | Controls testing, third?party audit reports             |
| <b>NIST CSF</b>      | Cybersecurity framework (Identify, Protect, Detect, Respond, Recover)                                  | US federal agencies & private sector                    | Flexible, risk?based control set                        |

*Tip:* Map each framework to the organization's data flows to see where overlap exists—this reduces duplicated effort.

## 4. Governance Structure

### 4.1 Organizational Roles

| Role                                                | Core Responsibilities                                                                     |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Board of Directors</b>                           | Set risk appetite, approve security budget, receive high?level compliance reports.        |
| <b>Chief Information Security Officer (CISO)</b>    | Develop security strategy, oversee governance policies, coordinate compliance activities. |
| <b>Compliance Officer / Data Protection Officer</b> | Monitor regulatory changes, maintain evidence of compliance, manage audits.               |

# Introduction to Security Compliance and Governance

## Role

## Core Responsibilities

### IT / Security Operations

Implement technical controls, monitor alerts, conduct vulnerability management.

### Legal / Privacy Team

Interpret statutes, draft contracts, handle breach notifications.

### Business Unit Leaders

Ensure departmental processes align with security policies, report incidents.

## 4.2 Governance Artifacts

- **Security Policy Suite** – High-level policies (e.g., Acceptable Use, Data Classification).
- **Standard Operating Procedures (SOPs)** – Detailed steps for routine tasks (e.g., patch management).
- **Control Catalog** – Mapping of controls to frameworks (e.g., ISO