

Introduction to Security Compliance and Regulations

Introduction to Security Compliance and Regulations

Quick reference guide for students, auditors, and security professionals

1. What Is Security Compliance?

Aspect	Description
Definition	The practice of adhering to laws, standards, and policies that govern the protection of information assets.
Goal	Ensure confidentiality, integrity, and availability (CIA) of data while meeting legal and contractual obligations.
Scope	Can apply to an entire organization, specific business units, or individual systems and processes.
Outcome	Demonstrated due diligence, reduced risk of breaches, avoidance of fines, and increased stakeholder trust.

2. Why Compliance Matters

- Legal Requirement** – Failure to follow statutes can result in civil/criminal penalties.
 - Financial Impact** – Fines, remediation costs, and loss of revenue from reputational damage.
 - Customer Confidence** – Clients often demand proof of compliance before doing business.
 - Operational Benefits** – Standardized processes improve efficiency and incident response.
 - Competitive Advantage** – Certifications can be a market differentiator.
-

3. Core Components of a Compliance Program

Component	Key Activities
Governance	- Define roles & responsibilities (CISO, Data Protection Officer, etc.) - Establish policies and procedures
Risk Assessment	- Identify assets, threats, and vulnerabilities - Evaluate likelihood & impact

Introduction to Security Compliance and Regulations

Component	Key Activities
Control Implementation	• Deploy technical (firewalls, IDS/IPS, firewalls) and administrative (training, background checks) controls
Monitoring & Auditing	• Continuous security monitoring • Periodic internal & external audits
Incident Management	• Formal response plan, reporting, and root-cause analysis
Reporting & Documentation	• Maintain evidence of compliance (logs, reports, attestations)
Continuous Improvement	• Review findings, update controls, and retrain staff

4. Major Regulatory Frameworks (U.S. & International)

Regulation	Sector / Data Covered	Key Requirements	Enforcement Agency
HIPAA (Health Insurance Portability and Accountability Act)	Healthcare	Protect PHI, risk analysis, breach notification	HHS Office for Civil Rights
PCI DSS (Payment Card Industry Data Security Standard)	Payment processing	Cardholder data protection, quarterly scans	PCI Security Standards Council (self-assessed)
GLBA (Gramm-Leach-Bliley Act)	Financial services	Safeguards for nonpublic personal info	FTC, CFPB
FISMA (Federal Information Security Management Act)	Federal agencies	NIST-based controls, annual reporting	OMB & DHS
SOX (Sarbanes-Oxley Act)	Publicly traded companies	Internal controls over financial reporting	SEC
GDPR (General Data Protection Regulation)	EU residents' personal data	Consent, data-subject rights, DPO, breach reporting (72h)	EU Data Protection Authorities

Introduction to Security Compliance and Regulations

Regulation	Sector / Data Collection	Key Requirements	Enforcement Agency
CCPA/CPRA (California Consumer Privacy Act & Privacy Rights Act)	California residents	Consumer rights, opt?out, data inventory	California Attorney General
NIST CSF (Cybersecurity Framework)	All sectors (voluntary)	Identify?Protect?Detect?Respond?Recover	NIST (guidance)
ISO/IEC 27001	Global – any organization	ISMS implementation, risk treatment, continual improvement	Accredited certification bodies

Tip: Many organizations adopt **baseline controls** (e