Data Security and Compliance: Comprehensive Assignment Report

1. Types of Security Assets

Understanding and categorizing assets is essential for effective cybersecurity and compliance management. Each asset type requires specific protection strategies and risk assessments to ensure organizational security and regulatory compliance.

Asset Type	Description	Examples
Physical Assets	Tangible items supporting IT and business operations	Servers, laptops, routers, office buildings
Digital Assets	Electronic resources holding value or sensitive data	Databases, digital documents, credentials
People Assets	Human resources interacting with systems and data	Employees, contractors, administrators
Paper Assets	Physical documents with sensitive or business-critical info	Contracts, printed reports, invoices
Services	Outsourced/internal services supporting business or IT functions	Cloud storage, legal services, SaaS platforms
Software	Applications and operating systems for information processing	CRM tools, antivirus, operating systems

---

2. Security Domains

Security domains define the scope and focus of protection strategies for different types of assets. Each domain has unique objectives and methods, but all work together to create a comprehensive security posture.

Security Domain	Focus Area & Scope	Key Objectives & Examples
IT Security	Digital data and IT infrastructure	Prevent unauthorized access, use firewalls, manage user access
Information Security	All forms of information (digital, physical, verbal)	Ensure confidentiality, integrity, and availability of all data

Security Domain	Focus Area & Scope	Key Objectives & Examples
Cybersecurity	Digital threats in cyberspace (internet, networks, systems)	Prevent cyber attacks, use IDS, secure coding, vulnerability assessments
Operational Security	Processes for handling and protecting sensitive information	Limit access by role, monitor for leaks, enforce policies

Key Differences:

- IT Security is technology-centric, focusing on digital infrastructure1.
- Information Security is the broadest, covering all information types2.
- Cybersecurity is a subset of InfoSec, specializing in digital threats.
- Operational Security emphasizes human and procedural controls1.

---

3. Data Laws and Penalties

PCI DSS (Payment Card Industry Data Security Standard)

- **About:** Global standard for organizations handling credit card data.
- **Penalties:** Fines from $5,000 to $100,000+ per month; additional fines of $50–$90 per affected customer in a breach.
- **Other Consequences:** Loss of card processing privileges, lawsuits, reputational damage, increased fees.

ISO 27001 (Information Security Management)

- **About:** International standard for information security management systems (ISMS).
- **Penalties:** No direct fines, but non-compliance can lead to financial losses, legal costs, sector-specific fines, and reputational damage.
- **Other Consequences:** Operational disruptions, loss of customer trust, increased insurance premiums.

GDPR (General Data Protection Regulation, EU)

- **About:** EU regulation for protecting personal data of EU residents, applies globally to organizations processing EU data.

- **Penalties:** Up to €20 million or 4% of annual global turnover, whichever is higher.
- **Other Consequences:** Processing bans, mandatory data deletion, compensation claims, reputational harm.

DPDPA (Digital Personal Data Protection Act, India)

- **About:** India's law regulating digital personal data collection, processing, and storage.
- **Penalties:** Fines up to ₹250 crore (~$30 million) for breaches; up to ₹200 crore for notification failures; up to ₹50 crore for other violations.
- **Other Consequences:** Business disruption, mandatory corrective actions, reputational harm.

HIPAA (Health Insurance Portability and Accountability Act, US)

- **About:** US law protecting the privacy and security of health information.
- **Penalties:** Civil fines from $137 to $68,928 per violation; annual maximums up to $2,067,813 per violation type; criminal penalties up to $250,000 and 10 years imprisonment for intentional violations.
- **Other Consequences:** Legal settlements, corrective action plans, loss of trust, business disruption.

---

4. Summary Table: Data Law Non-Compliance

Law	Max Penalty/Fine	Other Consequences
PCI DSS	$5,000–$100,000+/month; $50–$90/customer	Loss of card processing, lawsuits, brand damage
ISO 27001	No set fine; sector fines, breach costs	Reputational loss, operational disruption
GDPR	€20M or 4% global turnover	Processing bans, compensation claims, data deletion
DPDPA India	₹250 crore (~$30M)	Business disruption, corrective actions
HIPAA	$137–$68,928/violation; $2M+/year	Settlements, corrective plans, loss of trust

---