Cybersecurity Frameworks and Regulations

🔐 Cybersecurity Frameworks and Standards

1. NIST Cybersecurity Framework (CSF)

- **What it is**: A voluntary framework developed by NIST to enhance cybersecurity risk management.
- **Who must comply**: Primarily critical infrastructure in the U.S., but widely adopted globally.
- **Key principles/controls**: Five core functions – Identify, Protect, Detect, Respond, Recover.
- **Penalties**: No direct penalties, but non-adherence can lead to increased breach risk.

---

2. ISO/IEC 27001

- **What it is**: An international standard for implementing an Information Security Management System (ISMS).
- **Who must comply**: Organizations pursuing certification to demonstrate security maturity.
- **Key principles/controls**: 114 controls across 14 domains, including access control and risk management.
- **Penalties**: No legal penalties, but certification loss can impact business.

---

3. CIS Controls

- **What it is**: A set of best practices developed by the Center for Internet Security to improve cybersecurity.
- **Who must comply**: Voluntary adoption by organizations for basic security.
- **Key principles/controls**: 18 critical controls covering inventory, secure configuration, and more.
- **Penalties**: None, but lack of implementation increases cyber risk.

---

4. PCI DSS (Payment Card Industry Data Security Standard)

- **What it is**: A standard for securing credit card data.
- **Who must comply**: All entities processing, storing, or transmitting payment card data.
- **Key principles/controls**: 12 requirements including encryption, access control, and monitoring.
- **Penalties**: Fines up to $100,000/month and loss of card processing ability.

---

5. COBIT (Control Objectives for Information and Related Technologies)

- **What it is**: A framework for IT governance and management.
- **Who must comply**: Organizations needing structured IT governance.
- **Key principles/controls**: Governance components like Evaluate, Direct, Monitor (EDM) and others.
- **Penalties**: No legal penalties, but vital for audit and governance.

---

6. SOC 2 Trust Principles

- **What it is**: A compliance framework based on trust service criteria for service providers.
- **Who must comply**: SaaS and cloud-based service organizations.
- **Key principles/controls**: Security, Availability, Processing Integrity, Confidentiality, and Privacy.
- **Penalties**: No legal enforcement, but non-compliance may damage client trust.

🛡️ Cybersecurity Regulations and Laws

1. GDPR (General Data Protection Regulation - Europe)

- **What it is**: EU regulation for data protection and privacy.
- **Who must comply**: Any entity processing EU citizens' data.
- **Key principles/controls**: Consent, transparency, data minimization, breach notification.
- **Penalties**: Up to EUR 20 million or 4% of annual global turnover.

---

2. HIPAA (Health Insurance Portability and Accountability Act - USA)

- **What it is**: U.S. law protecting healthcare information.
- **Who must comply**: Healthcare providers, insurers, and their associates.
- **Key principles/controls**: Privacy Rule, Security Rule, Breach Notification Rule.
- **Penalties**: Up to $1.5 million/year per violation type; criminal penalties possible.

---

3. CCPA (California Consumer Privacy Act)

- **What it is**: California law granting consumers control over personal data.
- **Who must comply**: Businesses meeting specific data/revenue thresholds.
- **Key principles/controls**: Right to know, delete, and opt-out of data sale.
- **Penalties**: $2,500–$7,500 per violation.

---

4. Nigerian Data Protection Act (NDPA)

- **What it is**: Nigeria's comprehensive data protection regulation.
- **Who must comply**: Any organization handling Nigerian citizens' data.
- **Key principles/controls**: Lawful processing, consent, data subject rights, breach reporting.
- **Penalties**: Up to NGN 10 million or 2% of gross revenue.

---

5. SOX (Sarbanes-Oxley Act - USA)

- **What it is**: U.S. legislation ensuring corporate financial transparency.
- **Who must comply**: U.S. public companies and foreign firms listed on U.S. exchanges.
- **Key principles/controls**: Internal control over financial reporting.
- **Penalties**: Fines and imprisonment for executives violating the Act.

---

6. Nigerian Cybercrime Act 2015

- **What it is**: Nigeria's primary cybercrime legislation.
- **Who must comply**: All individuals and entities within Nigeria.

- **Key principles/controls**: Prohibits cyberstalking, fraud, system interference, unauthorized access.

- **Penalties**: Fines, imprisonment up to 10 years, asset seizure.
