🔐 Cybersecurity Frameworks & Standards

1. **NIST** Cybersecurity Framework (CSF) – USA

Developed by: National Institute of Standards and Technology (NIST)

Purpose: Provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks.

Core Functions: Identify, Protect, Detect, Respond, Recover

Applicability: Widely used across industries, including critical infrastructure.

2. **ISO/IEC 27001** – International

Published by: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Purpose: Specifies requirements for an Information Security Management System (ISMS)

Key Areas: Risk management, security controls, continual improvement

Applicability: Suitable for all types of organizations

3. **CIS Controls**

Developed by: Center for Internet Security (CIS)

Purpose: Provides prioritized cybersecurity best practices

Structure: 18 controls covering areas like inventory management, access control, and incident response

Applicability: Useful for both small and large organizations seeking practical, actionable guidance

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

Developed by: PCI Security Standards Council

Purpose: Designed to secure credit card transactions and cardholder data

Requirements: 12 core requirements including firewall use, access control, encryption, etc.

Applicability: Mandatory for all organizations handling cardholder information

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

Developed by: ISACA

Purpose: Provides a framework for IT governance and management

Focus: Aligning IT goals with business goals, managing risk, and ensuring compliance

Applicability: Widely used in corporate environments for IT control and audit

6. **SOC 2 Trust Principles**

Developed by: AICPA (American Institute of Certified Public Accountants)

Purpose: Ensures service providers manage data based on five “trust principles”:

Security

Availability

Processing Integrity

Confidentiality

Privacy

Applicability: Common among SaaS and cloud providers

📜 **Cybersecurity Laws & Data Protection Regulations**

1. GDPR (General Data Protection Regulation) – Europe

Enforced by: European Union

Purpose: Protects personal data and privacy of EU residents

Key Concepts: Consent, data subject rights, data breach notifications

Penalty: Up to €20 million or 4% of global revenue

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

Enforced by: U.S. Department of Health and Human Services

Focus: Protects health information (PHI) of individuals

Applicability: Healthcare providers, insurers, and their business associates

3. **CCPA** (California Consumer Privacy Act) – California, USA

Purpose: Grants California residents rights over their personal information

Key Provisions: Right to know, delete, and opt out of data selling

Applicability: Applies to for-profit businesses meeting certain criteria

4. **Nigerian Data Protection Act** (NDPA) – Nigeria

Enforced by: Nigeria Data Protection Commission (NDPC)

Purpose: Governs the collection, storage, and processing of personal data in Nigeria

Key Elements: Data subject rights, data controller obligations, penalties for breaches

5. **SOX** (Sarbanes-Oxley Act) – USA

Enforced by: U.S. Securities and Exchange Commission (SEC)

Purpose: Prevents fraud and financial misreporting in publicly traded companies

Relevance to Cybersecurity: Requires IT systems that ensure secure, accurate financial records

6. **Nigerian Cybercrime Act 2015**

Purpose: Criminalizes a wide range of cyber offenses including:

Hacking

Identity theft

Online fraud

Cyberstalking

Penalties: Fines and imprisonment depending on severity.

Who Must Comply:

Any organization (within or outside the EU) that processes the personal data of individuals in the EU.

Includes businesses, governments, nonprofits, and even non-EU companies offering goods/services or monitoring behavior in the EU.

Key Principles / Controls:

1. Lawfulness, Fairness, and Transparency – Data must be processed legally and transparently.

2. Purpose Limitation – Data collected for specific purposes must not be used for unrelated ones.

3. Data Minimization – Collect only the data that is necessary.

4. Accuracy – Keep data accurate and up to date.

5. Storage Limitation – Don’t keep personal data longer than needed.

6. Integrity and Confidentiality – Ensure data security.

7. Accountability – Organizations must demonstrate compliance.

Controls include:

Data Protection Impact Assessments (DPIAs)

Appointment of a Data Protection Officer (DPO) for some organizations

Breach notification within 72 hours

Consent management for data processing

Right to access, rectify, delete, and port personal data

Penalties for Non-Compliance:

Up to €20 million or 4% of annual global turnover, whichever is higher.

Lesser fines (up to 2%) for issues like record-keeping or lack of breach notification.

Real-life Example:

In 2021, Amazon was fined €746 million by Luxembourg’s National Commission for Data Protection (CNPD) for processing personal data in violation of GDPR – the largest GDPR fine to date.

Framework Mapping Recommendation for Nigerian Fintech Startup

Recommended Framework:

ISO/IEC 27001 – Information Security Management System (ISMS)

Why ISO 27001?

Global standard for managing information security risks.

Helps protect financial data, personal data, and IT infrastructure.

Provides a risk-based approach to identify, assess, and mitigate security threats.

Recognized across both Nigeria and Europe.

Key Controls:

Access control and encryption

Continuous risk assessments

Incident response procedures

Secure software development practices

Employee training and security awareness

Required Regulations to Comply With:

1. Nigerian Data Protection Act (NDPA)

Governs how personal data of Nigerians is collected, processed, and stored.

Applies to all Nigerian companies handling personal data.

Key Requirements:

Lawful and fair processing

Consent for data collection

Data minimization

Breach notification

Overseen by Nigeria Data Protection Commission (NDPC)

2. General Data Protection Regulation (GDPR) – Europe

Will apply as soon as the company begins handling personal data of EU residents.

Very strict rules on:

Consent

Right to be forgotten

Data portability

Breach notifications within 72 hours

Heavy fines (up to €20 million or 4% of global revenue)

ISO 27001 helps implement security controls that ensure data confidentiality, integrity, and availability, which are core to both NDPA and GDPR.

It also enforces documentation, audits, and accountability, which are key for compliance evidence.

As your cyber security I recommend adopting the ISO/IEC 27001 framework immediately. It's globally recognized and will build a strong information security posture that helps you meet Nigeria's NDPA now, and GDPR requirements when expanding into Europe.

4

1. Which standard is mandatory for credit card companies?
✅ PCI DSS (Payment Card Industry Data Security Standard) is mandatory for organizations that handle credit card transactions.

2. What does “CIA triad” stand for?
✅ Confidentiality, Integrity, Availability – the three core principles of cybersecurity.

3. GDPR fines can be up to what percentage of annual revenue?
✅ Up to 4% of annual global turnover (or €20 million, whichever is higher).

4. Which framework is published by NIST?
✅ The NIST Cybersecurity Framework (CSF) – developed by the U.S. National Institute of Standards and Technology.

5. Name one Nigerian cybersecurity law.
✅ Cybercrime (Prohibition, Prevention, etc.) Act, 2015

Great! Here's a clear and organized response to your request. I’ll break it down into two parts:

📊 1. Slides for the Chosen Frameworks/Regulations

You can copy these into PowerPoint, Google Slides, or Canva. Each slide has a title and brief bullet points.

Slide 1: NIST Cybersecurity Framework (CSF) Overview

- Developed by the U.S. National Institute of Standards and Technology
- Voluntary framework for managing cybersecurity risk
- Based on 5 core functions: Identify, Protect, Detect, Respond, Recover
- Widely used by private and public sectors globally

Slide 2: ISO/IEC 27001 Overview

- International standard for Information Security Management Systems (ISMS)
- Focuses on confidentiality, integrity, and availability (CIA Triad)
- Risk-based approach: assess, treat, monitor, and review risks

- Certification helps prove compliance and security maturity
- Supports GDPR and NDPA compliance

Slide 3: GDPR (General Data Protection Regulation)

- EU regulation on personal data protection
- Applies to any company handling EU residents' data
- Key rights: consent, access, rectification, erasure
- Mandatory breach reporting (within 72 hours)
- Fines: Up to €20 million or 4% of annual global revenue

Slide 4: Nigerian Cybercrime Act, 2015

- Enforces laws on cybercrime, identity theft, online fraud, and hacking
- Criminalizes unauthorised access, cyberstalking, cyberbullying
- Supports law enforcement and cybersecurity governance
- Penalties include fines and imprisonment
- Important for fintech and online platforms operating in Nigeria

---

📝 2. Short Report: Framework Mapping for Fintech Scenario

Scenario Summary

A Nigerian fintech startup is handling sensitive financial and personal data. With plans to expand to Europe, it must ensure cybersecurity and compliance with local and international data protection laws.

Recommended Framework

ISO/IEC 27001 – Provides a strong, certifiable structure for securing data and managing cyber risks.

- Globally recognized, including in Europe and Nigeria
- Builds a strong Information Security Management System (ISMS)
- Complements regulatory requirements from GDPR and NDPA

- Helps prevent breaches and ensure accountability

Relevant Regulations

1. NDPA (Nigerian Data Protection Act, 2023)

- Governs personal data handling in Nigeria
- Requires lawful processing, consent, security, and breach notification

2. GDPR (General Data Protection Regulation)

- Applies to any organization processing EU residents' data
- Requires strong privacy controls, data rights, and transparency

---

How Framework Supports Compliance

By adopting ISO 27001, the fintech company ensures a robust cybersecurity foundation that aligns with local and global data protection regulations