Cyber Security Frameworks, Standards and Regulations

NIST (National Institute of Standards and Technology)

- A non-regulatory agency of the United States Department of Commerce.
  - **Develop and publish cyber security standards, guidelines, and frameworks** (e.g., NIST Cyber security Framework, etc).
  - Provide guidance and resources for implementing cyber security best practices.
  - Conduct research and development in cyber security and related fields
  - Collaborate with industry, government, and academia to advance cyber security.
  - **Certification bodies, like the American National Standards Institute (ANSI), offer certifications based on NIST standards**

ISO (International Organization for Standardization)

- ISO is an independent, non-governmental organization that **develops and publishes international standards for** various industries, including technology and **cyber security.**
  - **Develops and publishes standards** (e.g., ISO 27001, ISO 27002) through a consensus-based process.
  - Provides **guidelines and requirements for implementing best practices.**
  - **Accredits certification bodies (CBs)** to audit and certify organizations against ISO standards
  - **Certification bodies, like SGS audit organizations and issue certifications (e.g., ISO 27001 certification) upon successful implementation of ISO standards**.

Cyber Security Frameworks, Standards and Regulations

- Frameworks: A structured approach or **set of guidelines for managing and implementing cyber security practices**.- Provide a broad outline of **best practices**, principles, and concepts.- Often flexible and adaptable to various organizations and industries.
  - Example:- NIST Cyber security Framework: A framework that provides a structured approach to managing cyber security, including five core functions (**Identify, Protect, Detect, Respond, Recover**).
  - CIS Controls Framework: A set of best practices for securing IT systems, (e.g., inventory management, vulnerability management).

Cyber Security Frameworks, Standards and Regulations

- Standards: A set of **specific requirements** for a particular aspect of cyber security.- Often used as a benchmark for evaluating cyber security practices.
  - Password standard: "Passwords must be at least 12 characters long and expire every 90 days.
  - Encryption standard: "All sensitive data must be encrypted using AES-256."

Cyber Security Frameworks, Standards and Regulations

- Standards: A set of **specific requirements** for a particular aspect of cyber security.- Often used as a benchmark for evaluating cyber security practices.
  - ISO 27001: A standard that provides requirements for an Information Security Management System (ISMS)
  - ISO 27002: A standard that provides guidelines for implementing information security controls.

Cyber Security Frameworks, Standards and Regulations

- In the context of cyber security, ISO 27001 serves as both a standard and a framework
  - Standard: It provides specific requirements for an Information Security Management System (ISMS)
  - Framework: It includes a structured approach and guidelines for implementing and managing an ISMS.

Cyber Security Frameworks, Standards and Regulations

- Standards: A set of **specific requirements** for a particular aspect of cyber security.- Often used as a benchmark for evaluating cyber security practices.
  - FIPS 140: The 140 series of Federal Information Processing Standards (FIPS) are U.S. government computer security standards that specify requirements for cryptography modules.

Cyber Security Frameworks, Standards and Regulations

- Standards: A set of **specific requirements** for a particular aspect of cyber security.- Often used as a benchmark for evaluating cyber security practices.
  - PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) to protect cardholder data and reduce credit card fraud. It ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Cyber Security Frameworks, Standards and Regulations

- Regulations:- Laws/legal requirements that **mandate specific cyber security controls** Typically apply to specific industries or sectors.
  - GDPR (General Data Protection Regulation): A European Union law that sets out the requirements for collecting, storing, and processing personal data. It requires organizations to implement specific data protection controls to protect personal data of EU citizens

Cyber Security Frameworks, Standards and Regulations

- Regulations:- Laws/legal requirements that **mandate specific cyber security controls** Typically apply to specific industries or sectors.
  - HIPAA (Health Insurance Portability and Accountability Act): A regulation that requires healthcare organizations to implement specific security controls and practices to protect patient data..

Cyber Security Frameworks, Standards and Regulations

- Regulations:- Laws/legal requirements that **mandate specific cyber security controls** Typically apply to specific industries or sectors.
  - Data Protection Act (DPA): A law in the UK regulating personal data handling, requiring organizations to inform customers about their data handling practices and provide a way for customers to access and delete their data.

Cyber Security Frameworks, Standards and Regulations

- Summary
  - Standards provide specific requirements (e.g., password length, encryption algorithm)
  - Frameworks provide a structured approach (e.g., NIST Cyber security Framework, CIS Controls)
  - Regulations are legal requirements (e.g., GDPR, HIPAA).