Security Frameworks

1. Introduction

Security frameworks provide structured and standardized guidelines that help organizations manage cybersecurity risks effectively. They enable organizations to identify threats, protect critical assets, detect security incidents, respond to attacks, and recover from disruptions. By adopting security frameworks, organizations can ensure regulatory compliance, improve security posture, and align cybersecurity initiatives with business objectives.

In modern enterprises, security frameworks also serve as a common language between technical teams, management, and regulatory bodies, ensuring consistent and measurable security practices.

2. NIST Cybersecurity Framework (CSF)

The **NIST Cybersecurity Framework (CSF)** is a widely adopted, risk-based framework developed by the National Institute of Standards and Technology. It provides a flexible and scalable approach to managing cybersecurity risks across organizations of all sizes and sectors.

Purpose of NIST CSF

- Improve critical infrastructure cybersecurity
- Provide a common structure for managing cyber risk
- Support continuous improvement in security programs

2.1 Five Core Functions of NIST CSF

Identify

The Identify function helps organizations understand their environment and manage cybersecurity risk.

Key Activities:

- Asset inventory and classification

- Business environment understanding
- Governance and risk assessment
- Supply chain risk management

Example:
An organization maintains an updated list of servers, endpoints, applications, and data assets to understand what needs protection.

Protect

The Protect function focuses on implementing safeguards to limit the impact of potential cybersecurity incidents.

Key Activities:

- Access control and identity management
- Security awareness and training
- Data protection and encryption
- Secure configuration and patch management

Example:
Applying security patches and enforcing strong authentication policies to prevent unauthorized access.

Detect

The Detect function enables timely discovery of cybersecurity incidents.

Key Activities:

- Continuous monitoring
- Log collection and analysis
- Anomaly and event detection
- SIEM implementation

Example:
Using SIEM tools to monitor unusual login activity or malware behavior.

Respond

The Respond function focuses on taking action after a cybersecurity incident is detected.

Key Activities:

- Incident response planning
- Communication and reporting
- Containment and mitigation
- Forensic analysis

Example:
Isolating infected systems and notifying stakeholders during a ransomware attack.

Recover

The Recover function supports restoration of services and systems following a cybersecurity incident.

Key Activities:

- Backup restoration
- System rebuilding
- Recovery planning
- Lessons learned and improvements

Example:
Restoring systems from clean backups and strengthening security controls after an incident.

3. ISO/IEC 27001

ISO/IEC 27001 is an international standard that defines the requirements for establishing, implementing, maintaining, and continually improving an **Information Security Management System (ISMS)**.

Purpose of ISO 27001

- Protect confidentiality, integrity, and availability of information
- Reduce information security risks
- Ensure compliance with legal and regulatory requirements

ISO 27001 follows a **risk-based approach**, ensuring that security controls are selected and implemented based on organizational risk assessments.

3.1 Key ISO 27001 Control Domains

Asset Management

Ensures that information assets are identified, classified, and protected appropriately.

Access Control

Defines policies to ensure only authorized users can access systems and data.

Cryptography

Ensures the secure use of encryption to protect sensitive information.

Operations Security

Focuses on secure system operations, change management, and malware protection.

Incident Management

Establishes procedures for reporting and responding to security incidents.

Business Continuity

Ensures information security is maintained during disruptions or disasters.

3.2 Continuous Improvement in ISO 27001

ISO 27001 follows the **Plan–Do–Check–Act (PDCA)** cycle:

- **Plan:** Identify risks and define controls
- **Do:** Implement security controls
- **Check:** Monitor and review effectiveness
- **Act:** Improve security posture

This cycle ensures continuous enhancement of the ISMS.

4. Case Study – WannaCry Ransomware

The **WannaCry ransomware attack (2017)** exploited unpatched SMB vulnerabilities in Microsoft Windows systems, causing widespread disruption across multiple organizations globally.

Impact of WannaCry

- Encrypted critical systems
- Disrupted healthcare and public services
- Highlighted the importance of patch management and backups

NIST FUNCTION	OBSERVATION
Identify	Unpatched systems
Protect	SMBv1 enabled
Detect	No malware alerts
Respond	Delayed response
Recover	Backup restoration required

5. Benefits of Using Security Frameworks

- Improved risk management
- Standardized security practices
- Regulatory and compliance support
- Enhanced incident response readiness
- Better communication between technical and management teams

6. Conclusion

Security frameworks such as NIST CSF and ISO/IEC 27001 play a vital role in building robust and resilient cybersecurity programs. By providing structured guidance, these frameworks help organizations manage risks effectively, respond to incidents efficiently, and align cybersecurity initiatives with business objectives. The WannaCry case study clearly demonstrates how gaps in framework implementation can lead to significant security failures, emphasizing the importance of adopting and maintaining strong security frameworks.