Security Frameworks

1. NIST Cybersecurity Framework (CSF)

NIST CSF provides a structured approach to managing cybersecurity risks.

Five Core Functions:

1. Identify – Asset management, risk assessment
2. Protect – Access control, encryption
3. Detect – Monitoring, anomaly detection
4. Respond – Incident handling
5. Recover – Restoration and improvements

2. ISO/IEC 27001

ISO 27001 is an international standard for information security management systems.

Key Domains:

- Asset Management
- Access Control
- Cryptography
- Operations Security
- Incident Management
- Business Continuity

3. Case Study: WannaCry Ransomware

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