

Assignment support: Cybersecurity challenges and Frameworks

**Dr. Thayananthan (Retired
professor)**

The Cybersecurity Framework

Three Primary Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources **using** the desired outcomes of the Framework Core

Implementation Tiers

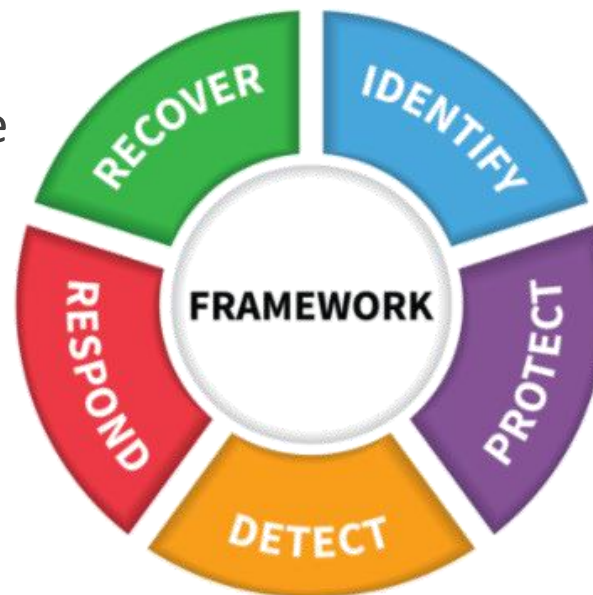
A qualitative measure of organizational cybersecurity risk management practices



Key Framework Attributes

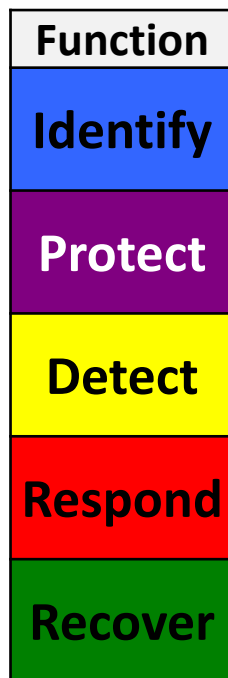
Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



The Framework Core

Establishes a Common Language



- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction



Implementation Tiers

The Cybersecurity Framework Version 1.1

	1	2	3	4
	Partial	Risk Informed	Repeatable	Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • monitors and manages supply chain risk^{1.1} • benefits my sharing or receiving information from outside parties			



Framework Update

The Cybersecurity Framework Version 1.1

- Applicability for all system lifecycle phases
- Enhanced guidance for managing cybersecurity within supply chains and for buying decisions
- New guidance for self-assessment
- Better accounts for Authorization, Authentication, and Identity Proofing
- Incorporates emerging vulnerability information (a.k.a., Coordinated Vulnerability Disclosure)
- Administratively updates the Informative References



CW: Synthesize a solution to a potential real-life scenario

- The shift to hybrid work models and reliance on cloud services
- Financial services firms like Vigilant Trust & Asset Management (VTAM)
- Protecting sensitive data and critical infrastructure from both external and internal threats.
- Modern security framework based on a Zero Trust approach.
- Credible sources (e.g., CISA, NIST, ENISA) and an appropriate diagram with frameworks such as those used in NIST or ISO 27001



Task 1: Identification of Modern Threats

- Internal and external threats (current and emerging)
- Ransomware-as-a-Service (RaaS)
- AI-powered social engineering (vishing)
- Supply chain compromises, and
- Risks associated with cloud adoption and hybrid work



Task 2: Modern Security Policies

- Understanding the security policies used in the frameworks
- Modern framework based on the Zero Trust model
- Applying policies to the cyber risks and threats with best practices learned from frameworks like NIST CSF and ISO 27001



Task 3: Technical Mitigation Measures

- Identified technical risks, threats and attacks for business and data management
- Mitigating technical risks, threats and attacks with MFA, SIEM and CSPM
- Proposing specific, feasible technical and administrative measures with the policies and frameworks
- Strategic investment in resilience for business continuity with the proposed approach



Task 4: Proactive Monitoring and Incident Response

- Proactive monitoring of risks
 - Outline a plan for 24/7 monitoring,
 - Threat detection methods with tools and policies
 - Incident Response with modern tools like SIEM and SOAR.
 - A flow chart or diagram of proactive monitoring.
-
- What is SIEM? | A Definition from TechTarget.com
 - <https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM>



Task 5: Continuous Training and Awareness

- Describe an engaging, continuous training program for improving the security management in IT sectors
- Explain the modern attack simulations (phishing/vishing)
- To handle the security issues, promote a culture of security awareness with your proposed approach



Presentation: Technical risks into business impacts

- Financial impact
 - Threat: Ransomware attack
 - Impact (Profit): - Good security (choose the best) with the policies (NIST/ISO/other) and mitigation or proactive plans or training.
 - Reduced risk of financial loss:
 - Increased stakeholder confidence:
 - Operational stability: Cost-effective risk management:
 - Comments with your proposed approach (your proposed solution)
- Operational impact
- Reputational impact
- Strategic investment in resilience



Any questions

- Please contact me to my email address:
 - v.thayananthan@uwtsd.ac.uk

