Cyber Audit

(Mapping the IT security policy framework definition to the seven domains of typical IT infrastructure)

By –Prakash Khasor,
Assistant Professor(Cyber Security),
National Forensic Sciences University

1. User Domain:

- Definition: This domain includes all individuals who access the organization's information system.

- Security Policy Mapping: Policies in this domain focus on user authentication, access controls, password policies, and user awareness training.

2. Workstation Domain:

- Definition: This domain includes all individual devices (desktops, laptops, etc.) connected to the organization's network.
- Security Policy Mapping: Policies address endpoint security, antivirus measures, system patching, and configurations to secure workstations.

.

3. LAN (Local Area Network) Domain:

- Definition: This domain involves the network infrastructure connecting workstations, servers, and other devices within a limited geographic area.

- Security Policy Mapping: Policies cover network segmentation, access controls, intrusion detection and prevention, and measures to secure the LAN.

4. LAN-to-WAN (Wide Area Network) Domain:

- Definition: This domain encompasses the connections between the organization's internal network and external networks (e.g., the Internet).
- Security Policy Mapping: Policies include firewall configurations, VPN usage, and measures to secure data in transit between the LAN and WAN.

5. WAN Domain:

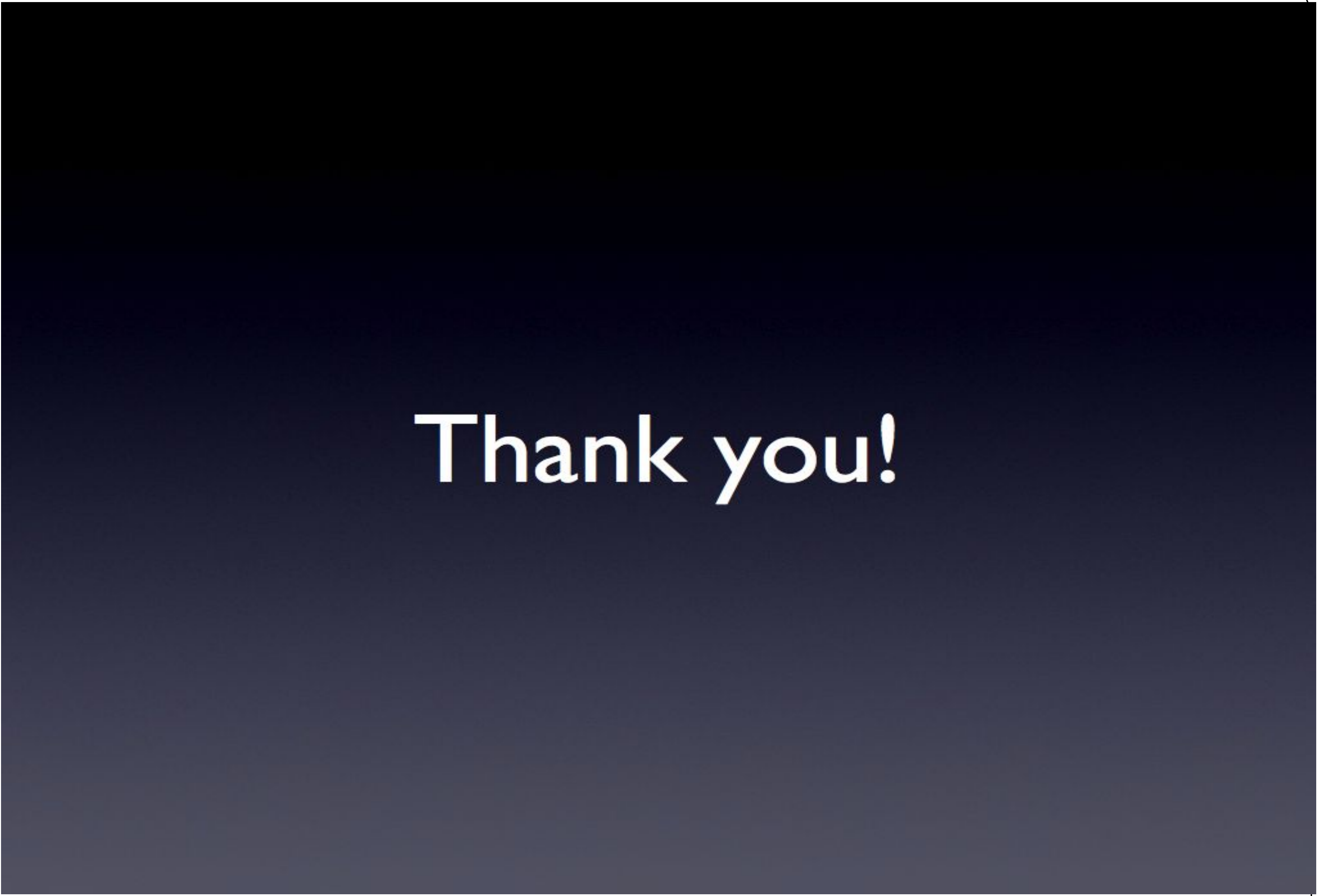
- Definition: This domain involves the wide area network that connects multiple LANs over a larger geographic area.
- Security Policy Mapping: Policies address secure data transmission, encryption for data in transit, and measures to protect the organization's data as it traverses the WAN.

6. System/Application Domain:

- Definition: This domain includes servers, databases, and applications that support business processes.
- Security Policy Mapping: Policies focus on access controls, data integrity, secure coding practices, and measures to protect against unauthorized access or data breaches.
- Patches
- unrestricted workstation access and untrusted software
- Email
- Social Engineering
- Antivirus Protection

7. Remote Access Domain:

- Definition: This domain covers the connections made to the organization's network by remote users or remote offices.
- Security Policy Mapping: Policies include secure remote access protocols, multi-factor authentication, and measures to ensure the security of data accessed remotely.
- Weak password
- Weak policy
- Lockout and History of Password
- Remote protocol set up and FTP , VPN



Thank you!