Lab #9 – Assessment Worksheet
Part A – Risks, Threats, & Vulnerabilities in the Seven Domains of a Typical IT Infrastructure

Course Name: IAP401
Student Name: Dang Hoang Nguyen

Risk – Threat – Vulnerability	**Primary Domain Impacted**
Unauthorized access from public Internet	Remote access Domain
User destroys data in application and **deletes all files**	System/Application Domain
Hacker penetrates your IT infrastructure and gains access to your **internal network**	LAN to WAN Domain
Intra-office employee romance gone bad	User Domain
Fire destroys primary **data center**	System/Application Domain
Communication circuit outages	WAN Domain
Workstation OS has a known **software vulnerability**	Workstation Domain
Unauthorized access to organization owned **Workstations**	Workstation Domain
Loss of production **data**	System/Application Domain
Denial of service attack on organization e-mail Server	LAN to WAN Domain
Remote communications from home office	Remote Access Domain
LAN server OS has a **known software vulnerability**	LAN Domain
User downloads an unknown e –mail attachment	User Domain
Workstation browser has software vulnerability	Workstation Domain
Service provider has **a major network** outage	WAN Domain
Weak ingress/egress traffic filtering degrades **Performance**	LAN to WAN Domain
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User Domain

VPN tunneling between **remote computer** and **ingress/egress router**	LAN to WAN Domain
WLAN access points are needed for LAN connectivity **within a warehouse**	LAN Domain -1-
Need to **prevent rogue users** from unauthorized WLAN access	LAN Domain

Lab #9 – Assessment Worksheet
Part B – Sample IT Security Policy Framework Definition

Course Name: IAP401
Student Name: Dang Hoang Nguyen

Risk – Threat – Vulnerability	**IT Security Policy Definition**
Unauthorized access from public Internet	**Policy Statement:** It is totally forbidden to gain unauthorized access from the public Internet. All remote access to the IT infrastructure of the company needs to be duly permitted and securely authenticated using techniques that have been approved, like multi-factor authentication VPN connections. **Purpose/Objectives:** • Assure the IT infrastructure of the company is secure and reliable. • Prevent cyber risks and attacks that come from the public Internet. Safeguard confidential information and resources against illegal access and use. **Scope:** This policy applies to all users, employees, contractors, and third parties accessing the organization's IT systems and resources remotely from the public Internet. **Standards**: • Remote access requires the implementation of robust authentication methods, such as multi-factor authentication (MFA). • In order to protect data while it is being transmitted over the open Internet, encryption mechanisms like SSL/TLS need to be enforced.

	• Firewalls and access control lists need to be set up to prevent unwanted access attempts from the public Internet. Protocols: • Consistently examine and modify access control policies and configurations to accommodate new threats and weaknesses. • Perform recurring audits and security assessments to make sure the policy is being followed. • Train staff members on security awareness, emphasizing the need of following security procedures and the dangers of unauthorized access over public WiFi. Guidelines: • Keep an eye on network traffic and log files in case you notice any illegal or suspicious efforts to access data coming from the public Internet. • Use intrusion detection and prevention systems to instantly identify and stop efforts by unauthorized users to gain access.
User destroys data in application and **deletes all files**	Policy Statement: Users are prohibited from intentionally destroying data in applications and deleting files without proper authorization. Any unauthorized modification or deletion of data constitutes a serious violation of IT security policies and may result in disciplinary action. Purpose/Objectives: • Safeguard the integrity and availability of data stored within applications and file systems.

	• Prevent unauthorized data loss or destruction that could impact business operations and continuity. • Establish accountability and deterrence against malicious actions by users. Scope: This policy applies to all users, employees, contractors, and third parties with access to the organization's applications and file systems. Standards: • Role-based access controls must be implemented to restrict users' ability to modify or delete data based on their job responsibilities. • Data backup and recovery procedures must be in place to restore lost or corrupted data in the event of unauthorized deletion or modification. • Logging and monitoring mechanisms must be deployed to track user actions and detect unauthorized data manipulation. Procedures: • Regularly review access permissions and user privileges to ensure they align with business requirements and least privilege principles. • Implement data loss prevention (DLP) solutions to detect and prevent unauthorized data destruction or deletion. • Conduct regular security awareness training to educate users about the importance of data security and the consequences of unauthorized actions.

	Guidelines: - Enforce strong password policies and implement session management controls to prevent unauthorized access to applications and file systems. - Implement file integrity monitoring systems to detect and alert on unauthorized changes to critical files and configurations.
Hacker penetrates your IT infrastructure and gains access to your **internal network**	Policy Statement: - Quick action is required to minimize security breaches, lessen their effects, and resume regular business activities in the event that a hacker breaches the organization's IT infrastructure and gains unauthorized access to the internal network. The coordination of response activities and the execution of corrective actions are within the purview of the incident response team. Purpose/Objectives: • Recognize security breaches and take immediate action to reduce the impact on data integrity and business operations. • Stop the attacker's further illegal access and data espionage. • Maintain the chain of custody and preserve the evidence for forensic examination and court cases. Scope: - This policy applies to all employees, contractors, and third-party service providers involved in incident

	response and security incident management. Standards: • An incident response plan must be developed, documented, and regularly tested to ensure readiness to handle security incidents effectively. • Incident response procedures must include predefined steps for identifying, containing, eradicating, and recovering from security breaches. • Communication protocols must be established to notify stakeholders, including management, IT staff, and legal counsel, of security incidents and response actions. Protocols: • Call in the Incident Response Team and start the incident response process in accordance with the incident response plan that has been previously established. • Work together as a team to control the breach and look into the occurrence, as well as with outside partners and law enforcement. • Keep track of every step you take in the incident response process, such as gathering and analyzing evidence and carrying out cleanup operations. Guidelines: • To restrict the ability of attackers to move laterally within the internal network, implement access limits and network segmentation.

	• Keep an eye out for unusual activity and indicators of compromise in network traffic and endpoints to spot intrusions early. • Perform lessons learned sessions and post-event reviews to pinpoint problem areas and strengthen incident response capabilities.
Intra-office employee romance gone bad	• **Standard:** Implement a workplace conduct policy outlining expectations for professional behavior, relationships, and conflict resolution. • **Guideline:** Provide training on workplace ethics and interpersonal relationships to mitigate potential conflicts. • **Procedure:** Establish a process for reporting and addressing workplace conflicts, including mediation and disciplinary actions if necessary. • **Asset Identification:** Identify personnel and human resources as critical assets requiring protection. • **Classification Policy:** Classify personnel-related data as sensitive and restrict access to authorized personnel only.
Fire destroys primary **data center**	• **Standard:** Implement a disaster recovery plan (DRP) to ensure business continuity in the event of a data center outage. • **Guideline:** Conduct regular backups and offsite storage of critical data to facilitate recovery efforts. • **Procedure:** Define roles and responsibilities for executing the DRP, including data restoration and system recovery processes. • **Asset Identification:** Identify data center facilities and infrastructure

	as critical assets requiring protection. • **Classification Policy:** Classify data based on importance and criticality for prioritized recovery efforts.
Communication circuit outages	• **Standard:** Implement redundant communication circuits and failover mechanisms to minimize service disruptions. • **Guideline:** Regularly monitor communication circuits for performance and availability issues. • **Procedure:** Establish protocols for notifying stakeholders and coordinating with service providers to troubleshoot and resolve outages. • **Asset Identification:** Identify communication infrastructure and services as critical assets requiring protection. • **Classification Policy:** Classify communication circuits based on importance and impact on business operations.
Workstation OS has a known **software vulnerability**	• **Standard:** Implement a patch management policy to regularly update and patch operating systems and software. • **Guideline:** Monitor security advisories and vendor announcements for patches and updates. • **Procedure:** Schedule and deploy patches promptly to mitigate vulnerabilities and minimize the risk of exploitation. • **Asset Identification:** Identify workstations as critical assets requiring protection.

	• **Classification Policy:** Classify vulnerabilities based on severity and prioritize patching accordingly.
Unauthorized access to organization owned **Workstations**	• **Standard:** Implement access control measures, such as user authentication and privilege management, to prevent unauthorized access. • **Guideline:** Enforce strong password policies and implement multi-factor authentication where feasible. • **Procedure:** Monitor and audit user activity on workstations to detect and respond to unauthorized access attempts. • **Asset Identification:** Identify workstations and user accounts as critical assets requiring protection. • **Classification Policy:** Classify sensitive data accessed from workstations and restrict access based on need-to-know.
Loss of production **data**	• **Standard:** Implement data backup and recovery procedures to ensure the integrity and availability of production data. • **Guideline:** Regularly test data backup and recovery processes to verify their effectiveness. • **Procedure:** Establish protocols for data restoration in the event of data loss or corruption. • **Asset Identification:** Identify production data and storage systems as critical assets requiring protection. • **Classification Policy:** Classify production data based on importance and sensitivity for prioritized backup and recovery efforts.

Denial of service attack on organization e-mail Server	• **Standard:** Implement network security measures, such as firewalls and intrusion prevention systems, to detect and mitigate denial of service attacks. • **Guideline:** Monitor network traffic for signs of suspicious activity and anomalous patterns indicative of denial of service attacks. • **Procedure:** Activate incident response protocols to mitigate the impact of the attack and restore email services. • **Asset Identification:** Identify email server infrastructure as critical assets requiring protection. • **Classification Policy:** Classify email services as critical for business operations and prioritize their protection against denial of service attacks.
Remote communications from home office	• **Standard:** Implement secure remote access protocols, such as VPN, with strong encryption and authentication. • **Guideline:** Educate remote users on best practices for secure remote communication, including password hygiene and device security. • **Procedure:** Require remote users to use company-provided devices or secure personal devices for remote communication. • **Asset Identification:** Identify remote access infrastructure and endpoints as critical assets requiring protection. • **Classification Policy:** Classify remote communications based on sensitivity and ensure encryption and data protection measures are applied accordingly.

LAN server OS has a **known software vulnerability**	• **Standard:** Implement a patch management policy to regularly update and patch server operating systems and software. • **Guideline:** Monitor security advisories and vendor announcements for patches and updates. • **Procedure:** Schedule and deploy patches promptly to mitigate vulnerabilities and minimize the risk of exploitation. • **Asset Identification:** Identify LAN servers as critical assets requiring protection. • **Classification Policy:** Classify vulnerabilities based on severity and prioritize patching accordingly.
User downloads an unknown e –mail attachment	□ **Standard:** Implement email security controls, such as spam filters and antivirus scanning, to detect and block malicious email attachments. □ **Guideline:** Educate users on identifying and avoiding suspicious email attachments and phishing attempts. □ **Procedure:** Establish protocols for handling suspicious email attachments, including reporting to IT security for analysis. □ **Asset Identification:** Identify email systems and user devices as critical assets requiring protection. □ **Classification Policy:** Classify email attachments based on risk and enforce policies for safe handling and execution.
Workstation browser has software vulnerability	• **Standard:** Implement web browser security updates and patches regularly. • **Guideline:** Educate users on safe browsing habits and avoiding potentially malicious websites. • **Procedure:** Configure web browsers to block or warn about potentially harmful content and restrict browser extensions.

	• **Asset Identification:** Identify workstations and web browsers as critical assets requiring protection. • **Classification Policy:** Classify web browsing activities based on risk and enforce policies for safe browsing and content filtering.
Service provider has **a major network** outage	• Standard: Establish service level agreements (SLAs) with service providers to ensure availability and performance requirements. • Guideline: Maintain redundant network connections and failover mechanisms to mitigate the impact of service provider outages. • Procedure: Activate incident response protocols to communicate with the service provider and implement contingency plans to restore services. • Asset Identification: Identify network connections and service provider relationships as critical assets requiring protection. • Classification Policy: Classify network services based on importance and prioritize redundancy and resilience measures accordingly.
Weak ingress/egress traffic filtering degrades **Performance**	• **Standard:** Implement robust traffic filtering mechanisms at ingress and egress points to control and optimize network traffic. • **Guideline:** Regularly monitor network performance and conduct traffic analysis to identify and address performance degradation issues. • **Procedure:** Configure and maintain traffic filtering rules and policies to prioritize critical traffic

	and block or throttle non-essential traffic. • **Asset Identification:** Identify ingress and egress points, network devices, and traffic filtering tools as critical assets requiring protection. • **Classification Policy:** Classify network traffic based on importance and prioritize bandwidth allocation and traffic shaping accordingly.
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	• **Standard:** Prohibit the use of unauthorized external storage devices on organization-owned computers. • **Guideline:** Educate users on the risks of using unauthorized external storage devices and provide secure alternatives for transferring files. • **Procedure:** Implement endpoint security measures to detect and block unauthorized device connections and enforce compliance with policy. • **Asset Identification:** Identify organization-owned computers and external storage devices as critical assets requiring protection. • **Classification Policy:** Classify data stored on external storage devices based on sensitivity and restrict access and usage accordingly.
VPN tunneling between **remote computer** and **ingress/egress router**	• **Standard:** Implement secure VPN protocols and encryption to protect data transmitted between remote computers and the network. • **Guideline:** Configure VPN clients and routers to use strong authentication methods and encryption algorithms. • **Procedure:** Establish VPN access controls and monitor VPN connections for security

	compliance and unauthorized access attempts. • **Asset Identification:** Identify VPN endpoints, remote computers, and network infrastructure as critical assets requiring protection. • **Classification Policy:** Classify VPN traffic based on sensitivity and apply encryption and access controls accordingly.
WLAN access points are needed for LAN connectivity **within a warehouse**	• **Standard:** Deploy secure WLAN access points with strong encryption and authentication mechanisms to prevent unauthorized access. • **Guideline:** Perform site surveys and RF analysis to optimize WLAN coverage and minimize interference. • **Procedure:** Configure WLAN access points with secure settings, such as SSID hiding, MAC filtering, and WPA2-PSK encryption. • **Asset Identification:** Identify WLAN access points, warehouse LAN infrastructure, and wireless devices as critical assets requiring protection. • **Classification Policy:** Classify WLAN traffic based on importance and sensitivity, and enforce access controls and encryption to protect data transmission.
Need to **prevent rogue users** from unauthorized WLAN access	□ **Standard:** Implement network access control (NAC) mechanisms to authenticate and authorize devices before granting access to the WLAN. □ **Guideline:** Educate users on the importance of WLAN security and the risks associated with unauthorized access. □ **Procedure:** Monitor WLAN traffic for unauthorized devices and behavior, and

	take action to block or quarantine rogue users. □ **Asset Identification:** Identify WLAN infrastructure and devices as critical assets requiring protection. □ **Classification Policy:** Classify WLAN access based on user roles and privileges, and enforce access controls and authentication mechanisms to prevent unauthorized access

Lab #9 – Assessment Worksheet
Assess and Audit an Existing IT Security Policy Framework Definition

Course Name: IAP401

Student Name: Dang Hoang Nguyen

1. What is the purpose of having a policy framework definition as opposed to individual policies?

An organization's policy management can be done more methodically and cohesively with the help of a defined policy framework. Having unified policies, as opposed to fragmented, sometimes non-coherent policies, guarantees coherence, integration, and clarity in policy interpretation and execution.

2. When should you use a policy definition as a means of risk mitigation and element of a layered

When a policy definition covers specific security objectives and controls across different domains or areas of the company, it should be used as a tool for risk reduction and as part of a layered security strategy. This guarantees a thorough approach to risk management and improves security measure efficacy.

3. In your gap analysis of the IT security policy framework definition provided, which policy definition was missing for all access to various IT systems, applications, and data throughout the scenario?

An Access Control Policy is required for all access to different IT systems, applications, and data in the scenario, but it has not yet been defined. In order to guarantee that only those who are authorized have the proper access credentials, this policy lays out the guidelines and processes for assigning and monitoring access rights to organizational resources.

4. Do you need policies for your telecommunication and Internet service providers?

Yes, policies for internet service providers and telecommunications companies are required to set standards, obligations, and roles for guaranteeing the security and dependability of the services the company uses for internet and telecommunications.

5. Which policy definitions from the list provided in Lab #9 – Part B helps optimize performance of an organization's Internet connection?

The policy definition for "Weak ingress/egress traffic filtering degrades Performance" helps optimize the performance of an organization's Internet connection by addressing the need for effective ingress and egress traffic filtering to enhance network performance and security.

6. What is the purpose of a Vulnerability Assessment & Management Policy for an IT infrastructure?

Establishing guidelines and processes for locating, evaluating, prioritizing, and fixing vulnerabilities within the organization's systems and network infrastructure is the goal of a vulnerability assessment and management policy for an IT infrastructure. This lowers the possibility that malicious actors may exploit these vulnerabilities.

7. Which policy definition helps achieve availability goals for data recovery when data is lost or corrupted?

The policy definition for "Loss of production data" outlines methods and practices for data backup, restoration, and recovery to reduce downtime and maintain continuity of operations. This helps to accomplish availability targets for data recovery when data is lost or corrupted.

8. Which policy definitions reference a Data Classification Standard and use of cryptography for confidentiality purposes?
The terms "Data Protection Policy" and "Encryption Policy" refer to the usage of cryptography for confidentiality and a Data Classification Standard. These regulations specify criteria for sensitive data classification and provide instructions for encrypting confidential data to maintain confidentiality.

9. Which policy definitions from the sample IT security policy framework definition mitigate risk in the User Domain?
Acceptable Use Policy, User Authentication Policy, and User Training and Awareness Policy are some of the policy definitions from the example IT security policy framework definition that reduce risk in the User Domain.

10. Which policy definition from the sample IT security policy framework definition mitigates risk in the LAN-to-WAN Domain?
The sample IT security policy framework definition's Access Control Policy, which controls access to network resources and aids in preventing unwanted access and data breaches, is the policy definition that reduces risk in the LAN-to-WAN Domain.

11. How does an IT security policy framework make it easier to monitor and enforce throughout an
organization?
By offering a centralized framework for developing, updating, disseminating, and enforcing policies, an IT security policy framework facilitates monitoring and enforcement throughout the entire business. Stakeholders will find it easier to comprehend and abide by security standards as a result of its assurance of consistency, clarity, and connection with company goals.

12. Which policy definition requires an organization to list its mission critical business operations and functions and the accompanying IT systems, applications, and databases that support it?
Usually found in the Business Impact Analysis (BIA) Policy Definition, this policy definition mandates that an organization list its mission-critical business activities and services together with the supporting IT systems, databases, and applications.

13. Why is it common to find a Business Continuity Plan (BCP) Policy Definition and a Computer
Security Incident Response Team (CSIRT) Policy Definition?
A business's overall risk management and resilience plan often includes both a Computer Security Incident Response Team (CSIRT) policy definition and a Business Continuity Plan (BCP) policy definition. In the case of an interruption, BCP guarantees operations will continue, while CSIRT guarantees efficient reaction to and recovery from security problems.

14. True or False. A Data Classification Standard will define whether or not you need to encrypt the data while residing in a database.

True. A Data Classification Standard defines the sensitivity and criticality of data, which informs whether encryption is necessary based on the classification of the data.

15. True or False. Your upstream Internet Service Provider must be part of your Denial of Service /
Distributed Denial of Service risk mitigation strategy at the LAN-to-WAN Domain's Internet ingress/egress. This is best defined in a policy definition for Internet ingress/egress availability

Indeed. To ensure cooperation and coordination in preventing DDoS attacks and preserving Internet connectivity, it is best to include the upstream Internet Service Provider in the Denial of Service / Distributed Denial of Service risk mitigation strategy at the LAN-to-WAN Domain's Internet ingress/egress.