# Lab #9: Assess and Audit an Existing IT Security Policy Framework Definition

**Course Name:** Policy Development in Information Assurance (IAP301)
**Student Name:** Nguyễn Trần Vinh – SE160258
**Instructor Name:** Mai Hoàng Đỉnh
**Lab Due Date:** 28/10/2023

## Part A
## Risks, Threats, & Vulnerabilities in the Seven Domains of a Typical IT Infrastructure

### Overview
For each of the identified risks, threats, and vulnerabilities – review the following chart to determine which domain from the seven domains of a typical IT infrastructure is impacted

| Risk – Threat – Vulnerability | Primary Domain Impacted |
|---|---|
| Unauthorized access from public Internet | WAN 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, LAN Domain |
| Communication circuit outages | LAN-to-WAN Domain, WAN Domain |
| Workstation OS has a known software vulnerability | User 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, 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 | Remote Access Domain |
| WLAN access points are needed for LAN connectivity within a warehouse | LAN Domain |
| Need to prevent rogue users from unauthorized WLAN access | LAN Domain |

## Part B – Sample IT Security Policy Framework Definition

## Overview

Given the following IT security policy framework definition, specify which policy probably can cover the identified risk, threat, or vulnerability. If there is none, then identify that as a gap. Insert your recommendation for an IT security policy that can eliminate the gap.

| Risk – Threat – Vulnerability | IT Security Policy Definition |
|---|---|
| Unauthorized access from public Internet | Asset Protection Policy |
| User destroys data in application and deletes all files | Asset Management Policy |
| Hacker penetrates your IT infrastructure and gains access to your internal network | Threat Assessment & Management Policy, Vulnerability Assessment & Management Policy |
| Intra-office employee romance gone bad | Security Awareness Training Policy |
| Fire destroys primary data center | Asset Protection Policy |
| Communication circuit outages | Asset Protection Policy |
| Workstation OS has a known software vulnerability | Vulnerability Assessment & Management Policy |
| Unauthorized access to organization owned Workstations | Asset Identification & Classification Policy |
| Loss of production data | Asset Management Policy |
| Denial of service attack on organization e-mail Server | Threat Assessment & Management Policy |
| Remote communications from home office | Asset Protection Policy |
| LAN server OS has a known software vulnerability | Vulnerability Assessment & Management Policy |
| User downloads an unknown e-mail attachment | Security Awareness Training Policy |
| Workstation browser has software vulnerability | Vulnerability Assessment & Management Policy |
| Service provider has a major network outage | Asset Protection Policy |
| Weak ingress/egress traffic filtering degrades Performance | Threat Assessment & Management Policy |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | Asset Management Policy |
| VPN tunneling between remote computer and ingress/egress router | Asset Protection Policy |
| WLAN access points are needed for LAN connectivity within a warehouse | Asset Identification & Classification Policy |
| Need to prevent rogue users from unauthorized WLAN access | Asset Protection Policy |

**PART C**

## Overview

In this lab, you were presented with a list of common risks, threats, and vulnerabilities commonly found in the seven domains of a typical IT infrastructure. The students were presented with a sample IT security policy framework definition. Most of these policy definitions cover the identified risks, threats, and vulnerabilities. Some have gaps that must be mitigated with recommendations for other IT security policies. This lab demonstrated how to assess and audit an IT security policy framework definition by performing a gap analysis with remediation

## Lab Assessment Questions & Answers

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

Answer:

- It ensures consistency and alignment among individual policies. A well-defined policy framework will help to ensure that all of the organization's policies are aligned with its overall goals and objectives. It will also help to ensure that policies are consistent with each other and do not conflict with each other.
- It provides guidance for policy development. The policy framework definition should provide guidance to staff on how to develop and implement new policies. This can help to ensure that policies are well-thought-out and effective.
- It facilitates communication and understanding of policies. The policy framework definition can help to communicate the organization's overall approach to policy development and implementation to staff and other stakeholders. This can help to build understanding of and support for individual policies.

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

Answer:

- Provide a consistent and coherent approach to policy-making and implementation across your organization
- Align your policies with your organization's vision, mission, values, and strategic goals
- Respond to the changing needs and expectations of your stakeholders
- Coordinate and integrate your policies across different domains, levels, and functions of your organization
- Avoid duplication or contradiction of policies
- Monitor, evaluate, and review the effectiveness and impact of your policies over time
- Transfer the risk allocation between different parties
- Accept a certain risk for a certain period of time
- Avoid a certain risk that has too high consequences for your organization
- Monitor different processes and teams to assess risks as they happen

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?

Answer: **Access Control Policy**. An access control policy defines the rules and procedures for granting and denying access to IT systems, applications, and data. It is an essential policy for any organization that wants to protect its information assets from unauthorized access.

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

Answer: Yes, you may need policies for your telecommunication and Internet service providers, depending on your context and objectives. Policies are sets of rules or principles that guide the actions and decisions of an organization or a government. Policies can help to ensure the quality, security, affordability, and accessibility of telecommunication and Internet services for users and providers.

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

Answer:

- Asset Protection Policy: Implement a traffic filtering solution to block malicious traffic and improve performance.
- Vulnerability Assessment & Management Policy: Install security patches promptly to remediate known vulnerabilities in network devices and software.
- Threat Assessment & Management Policy: Implement a denial-of-service (DoS) mitigation plan to protect against DoS attacks.

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

- Identify assets: The first step is to identify all of the assets in the IT infrastructure, including hardware, software, and data.
- Assess vulnerabilities: Once the assets have been identified, they need to be assessed for vulnerabilities. This can be done using a variety of tools and techniques, including manual and automated vulnerability scanners.
- Prioritize vulnerabilities: Once the vulnerabilities have been identified, they need to be prioritized based on their severity and the potential impact to the organization.
- Remediate vulnerabilities: The final step is to remediate the vulnerabilities. This may involve applying patches, changing configurations, or implementing other security controls.

7. Which policy definition helps achieve availability goals for data recovery when data is lost or corrupted?
Answer: A data backup policy is most closely related to an **asset protection policy**, which is a document that defines the rules and procedures for safeguarding the physical and logical assets of an organization from unauthorized access, use, modification, disclosure, or destruction. An asset protection policy can cover various aspects of security, such as access control, encryption, authentication, logging, monitoring, incident response, and disaster recovery. A data backup policy can be considered as a subset or a component of an asset protection policy, focusing specifically on the backup and restoration of data.

8. Which policy definitions reference a Data Classification Standard and use of cryptography for confidentiality purposes?
Answer:

- **Asset Identification & Classification Policy**: This policy defines the rules and procedures for identifying and classifying the data and IT assets of an organization according to their sensitivity, criticality, and value. A Data Classification Standard is a framework for assessing the adverse impact that loss of data confidentiality, integrity, or availability would have upon the organization. A Data Classification Standard can help an organization to determine the appropriate level of protection and encryption for each type of data.
- **Asset Protection Policy**: This policy defines the rules and procedures for safeguarding the physical and logical assets of an organization from unauthorized access, use, modification, disclosure, or destruction. Cryptography is a major tool for providing data confidentiality, as well as data integrity and authentication. Cryptography is the study of mathematical techniques for the secure transmission of a private message over an insecure channel. Cryptography involves encrypting a message with a key and decrypting it with the same or a different key.
- **Security Awareness Training Policy**: This policy defines the rules and procedures for providing regular and effective training to the staff of an organization on the best practices and policies for information security. A Security Awareness Training Policy can help an organization to raise the awareness and competence of its staff on how to handle and protect sensitive data, how to use cryptography tools properly, and how to prevent or respond to security incidents.

9. Which policy definitions from the sample IT security policy framework definition mitigate risk in the User Domain?
Answer:

- **Security Awareness Training Policy**: This policy defines the rules and procedures for providing regular and effective training to the staff of an organization on the best practices and policies for information security. A Security Awareness Training Policy can help an organization to raise the awareness and competence of its staff on how to handle and protect sensitive data, how to use cryptography tools properly, and how to prevent or respond to security incidents.
- **Threat Assessment & Management Policy**: This policy defines the rules and procedures for identifying, analyzing, and responding to potential or actual threats to the IT infrastructure. A Threat Assessment &

Management Policy can help an organization to proactively detect and mitigate threats from internal or external sources, such as malicious users, hackers, malware, or natural disasters. A Threat Assessment & Management Policy can also include guidelines for reporting and escalating incidents, conducting investigations, and implementing corrective actions.

- **Asset Identification & Classification Policy**: This policy defines the rules and procedures for identifying and classifying the data and IT assets of an organization according to their sensitivity, criticality, and value. A Data Classification Standard is a framework for assessing the adverse impact that loss of data confidentiality, integrity, or availability would have upon the organization. A Data Classification Standard can help an organization to determine the appropriate level of protection and encryption for each type of data.

10. Which policy definition from the sample IT security policy framework definition mitigates risk in the LAN-to-WAN Domain?

Answer:

- **Asset Protection Policy**: This policy defines the rules and procedures for safeguarding the physical and logical assets of an organization from unauthorized access, use, modification, disclosure, or destruction. An Asset Protection Policy can cover various aspects of security, such as access control, encryption, authentication, logging, monitoring, incident response, and disaster recovery. An Asset Protection Policy can help an organization to protect its LAN-to-WAN devices, such as routers, firewalls, VPNs, and gateways, from unauthorized or malicious access or tampering. An Asset Protection Policy can also help an organization to encrypt and authenticate its LAN-to-WAN traffic to ensure data confidentiality and integrity.
- **Vulnerability Assessment & Management Policy**: This policy defines the rules and procedures for identifying, evaluating, applying, and verifying system updates to mitigate vulnerabilities in the IT environment and the risks associated with them. A vulnerability is a weakness or flaw in a system or application that can be exploited by an attacker to compromise the confidentiality, integrity, or availability of the system or data. A vulnerability assessment is a process of scanning, testing, and analyzing the IT environment to discover and report on existing vulnerabilities. A Vulnerability Assessment & Management Policy can help an organization to scan and test its LAN-to-WAN devices and connections for vulnerabilities and apply patches or other remediation measures to address them. A Vulnerability Assessment & Management Policy can also help an organization to monitor and report on its vulnerability status and compliance.

11. How does an IT security policy framework make it easier to monitor and enforce throughout an organization?

Answer:

- Provides a centralized view of all IT security policies: An IT security policy framework provides a single place where organizations can store and manage all of their IT security policies. This makes it easier to find and review policies, as well as to ensure that all policies are consistent and up-to-date.
- Defines roles and responsibilities for policy monitoring and enforcement: An IT security policy framework should define the roles and responsibilities of different stakeholders in the organization for monitoring and enforcing IT security policies. This helps to ensure that everyone knows what they are responsible for and that there is no accountability gap.
- Provides tools and resources for policy monitoring and enforcement: An IT security policy framework can provide tools and resources to help organizations monitor and enforce IT security policies. This may include tools for auditing system logs, detecting suspicious activity, and responding to security incidents.
- Facilitates communication and collaboration: An IT security policy framework can facilitate communication and collaboration between different stakeholders in the organization on IT security matters. This helps to ensure that everyone is on the same page and that policies are implemented and enforced effectively.

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?
Answer:

- The policy definition that requires an organization to list its mission critical business operations and functions and the accompanying IT systems, applications, and databases that support it is called a business impact analysis (BIA). A BIA is a key component of a business continuity plan, as it helps identify and prioritize the most essential business activities and the resources needed to sustain them. A BIA also evaluates the potential impact of various disruptions on the organization's operations, revenue, reputation, and legal obligations

13. Why is it common to find a Business Continuity Plan (BCP) Policy Definition and a Computer Security Incident Response Team (CSIRT) Policy Definition?
Answer:

- A BCP Policy Definition outlines the objectives, scope, roles, and responsibilities of a BCP, which is a strategy that helps organizations ensure they can still facilitate vital business operations through or despite downtime, attacks, or incidents. A CSIRT Policy Definition defines the purpose, scope, authority, and functions of a CSIRT, which is a capability set up for the purpose of assisting in responding to computer security-related incidents. Both policies help organizations prepare for, respond to, and recover from various types of cyber threats and incidents, as well as minimize the impact and damage on their operations, assets, and reputation.

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

- True. A Data Classification Standard and its associated policies typically define the requirements for data encryption, including whether or not data needs to be encrypted while residing in a database. Data classification is an important part of data lifecycle management that specifies which standard category or grouping a data object belongs in. Once sorted, data classification can help ensure an organization adheres to its own data handling guidelines and to local, state, and federal compliance regulations.

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.
Answer:

- True. Your upstream Internet Service Provider (ISP) must be part of your Denial of Service / Distributed Denial of Service (DoS/DDoS) 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. A policy definition is a document that specifies the goals, scope, roles, and responsibilities of a particular policy, such as a DoS/DDoS prevention policy. A policy definition for Internet ingress/egress availability would outline the objectives, expectations, and requirements for ensuring the availability and resilience of the network connection between the local area network (LAN) and the wide area network (WAN), especially in the event of a DoS/DDoS attack.