Laboratory #9

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

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify risks, threats, and vulnerabilities in the seven domains of a typical IT infrastructure
- Review existing IT security policies as part of a policy framework definition
- Align IT security policies throughout the seven domains of a typical IT infrastructure as part of a layered security strategy
- Identify gaps in the IT security policy framework definition
- Recommend other IT security policies that can help mitigate all known risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #9:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #9 – Student Steps:

The following represents the steps that must be followed for Lab #9 – Assess and Audit an Existing IT Security Policy Framework Definition:

1. Discuss the seven domains of a typical IT infrastructure
2. Discuss what risks, threats, and vulnerabilities are commonly found throughout the seven domains of a typical IT infrastructure
3. Review the Lab #9 – Assessment Worksheet, Part A – Risks, Threats, & Vulnerabilities Found in a Typical IT Infrastructure

4. Review the sample IT security policy framework provided in Lab #9 – Assessment Worksheet, Part B – Identify Gaps in a Given IT Security Policy Framework Definition
5. Review the list of IT security policy definitions that can help fill identified gaps in the IT security policy framework definition
6. Complete Lab #9 – Assessment Worksheet, Part B
7. Answer the Lab #9 – Assessment Questions & Answers

Deliverables

Upon completion of Lab #9: Assess and Audit an Existing IT Security Policy Framework Definition, students are required to provide the following deliverables as part of this lab:

1. Lab #9 – Assessment Worksheet, Part B – IT Security Policy Framework Gap Recommendations
2. Lab #9 – Assessment Worksheet questions and answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #9 – Assess and Audit an Existing IT Security Policy Framework Definition that the students must perform:

1. Was the student able to identify risks, threats, and vulnerabilities in the seven domains of a typical IT infrastructure? – [**20%**]
2. Was the student able to review existing IT security policies as part of a policy framework definition? – [**20%**]
3. Was the student able to align IT security policies throughout the seven domains of a typical IT infrastructure as part of a layered security strategy? – [**20%**]
4. Was the student able to identify gaps in the IT security policy framework definition? – [**20%**]
5. Was the student able to recommend other IT security policies that can help mitigate all known risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure? – [**20%**]

Lab #9 – Assessment Worksheet

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

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name: _____

Lab Due Date: _____

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	Workstation Domain
Hacker penetrates your IT infrastructure and gains access to your internal network	LAN Domain
Intra-office employee romance gone bad	User Domain
Fire destroys primary data center	System Application Domain
Communication circuit outages	System Application Domain
Workstation OS has a known software vulnerability	Workstation Domain
Unauthorized access to organization owned Workstations	LAN Domain
Loss of production data	System Application Domain
Denial of service attack on organization e-mail Server	System Application Domain
Remote communications from home office	Remote Access

Risk – Threat – Vulnerability	Primary Domain Impacted
LAN server OS has a known software vulnerability	LAN Domain
User downloads an unknown e –mail attachment	LAN Domain
Workstation browser has software vulnerability	User Domain
Service provider has a major network outage	WAN Domain
Weak ingress/egress traffic filtering degrades Performance	WAN Domain
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	Workstation Domain
VPN tunneling between remote computer and ingress/egress router	WAN Domain
WLAN access points are needed for LAN connectivity within a warehouse	LAN to WAN Domain
Need to prevent rogue users from unauthorized WLAN access	System Applications Domain

Lab #9 – Assessment Worksheet

Part B – Sample IT Security Policy Framework Definition

Course Name: IAP301

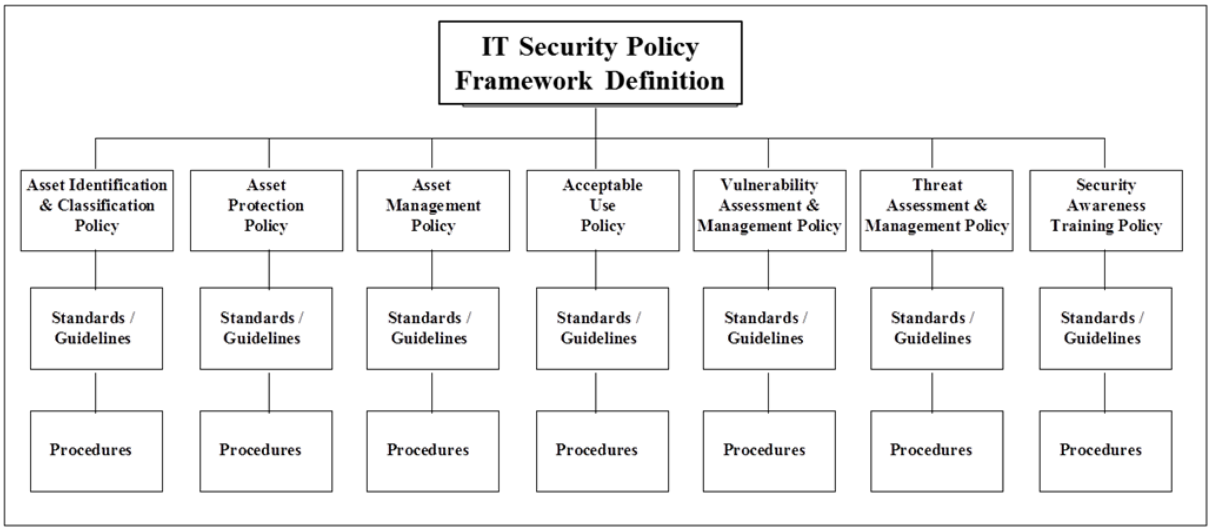
Student Name: Nguyễn Quốc Vượng

Instructor Name: _____

Lab Due Date: _____

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	Data Classification Standard & Encryption Policy
Hacker penetrates your IT infrastructure and gains access to your internal network	Vulnerability Assessment & Management Policy
Intra-office employee romance gone bad	Security Awareness Training Policy
Fire destroys primary data center	Business Continuity & Disaster Recovery Policy
Communication circuit outages	Business Continuity & Disaster Recovery Policy
Workstation OS has a known software vulnerability	Vulnerability Assessment & Management Policy
Unauthorized access to organization owned Workstations	Asset Protection Policy
Loss of production data	Business Continuity & Disaster Recovery 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	Business Continuity & Disaster Recovery Policy
Weak ingress/egress traffic filtering degrades performance	Asset Protection Policy
User inserts CDs and USB hard drives with personal photos, music, and videos	Asset Protection Policy

Risk – Threat – Vulnerability	IT Security Policy Definition
VPN tunneling between remote computer and ingress/egress router	Asset Protection Policy
WLAN access points are needed for LAN connectivity within a warehouse	Asset Protection Policy
Need to prevent rogue users from unauthorized WLAN access	Asset Protection Policy

For each identified gap, insert a recommendation for an IT security policy to help mitigate the risk, threat or vulnerability:

Lab #9 – Assessment Worksheet

Assess and Audit an Existing IT Security Policy Framework Definition

Course Name: IAP301

Student Name: Nguyễn Quốc Vương

Instructor Name: _____

Lab Due Date: _____

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?
   A policy framework ensures consistency and coherence across an organization by aligning individual policies with overarching principles and objectives. It provides comprehensive coverage, guiding the development and implementation of policies while identifying gaps and overlaps. This approach streamlines processes, enhances clarity, and establishes accountability and governance, making policies easier to manage and adapt. Additionally, it aids in risk management by evaluating all policies against common standards and objectives. Overall, a policy framework enhances the effectiveness and efficiency of organizational policies

2. When should you use a policy definition as a means of risk mitigation and element of a layered security strategy?
   You should use a policy definition for risk mitigation and as an element of a layered security strategy when you need to establish clear guidelines and procedures to protect against various threats, ensure compliance with regulations, and create a structured approach to security. This helps in addressing vulnerabilities systematically, setting standards for behavior and response, and providing a foundation for other security measures, thereby enhancing overall organizational resilience and reducing risk

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?

The missing policy definition in the gap analysis of the IT security policy framework was an Access Control Policy. This policy is essential for managing and regulating who can access various IT systems, applications, and data, ensuring that only authorized personnel have appropriate access rights to sensitive information and resources

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

Yes, you need policies for your telecommunication and Internet service providers to ensure secure and reliable communication channels, define service level expectations, manage risks, protect data integrity, and ensure compliance with legal and regulatory requirements. These policies help establish clear guidelines and standards for the providers, ensuring that they meet the organization's security and operational needs

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

The policy definitions from the list provided in Lab #9 – Part B that help optimize performance of an organization's Internet connection are the Bandwidth Management Policy and the Internet Usage Policy. The Bandwidth Management Policy should define the rules and priorities for allocating and regulating network bandwidth, while the Internet Usage Policy should establish guidelines and restrictions for accessing and using the Internet, such as acceptable use, prohibited activities, and monitoring

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

The purpose of a Vulnerability Assessment & Management Policy for an IT infrastructure is to identify, evaluate, and mitigate vulnerabilities in the system. This policy establishes a systematic approach for regularly scanning and assessing potential security weaknesses, prioritizing them based on risk, and implementing measures to remediate or manage these vulnerabilities. It aims to enhance the overall security posture of the organization, reduce the risk of breaches, and ensure continuous protection of IT assets

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

The Data Backup and Recovery Policy helps achieve availability goals for data recovery when data is lost or corrupted. This policy outlines procedures for regularly backing up data, storing backups securely, and defining processes for restoring data to ensure minimal disruption and quick recovery in the event of data loss or corruption

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

The Data Protection Policy and the Information Security Policy reference a Data Classification Standard and use of cryptography for confidentiality purposes. These policies outline how data should be classified based on sensitivity and importance, and specify the use of encryption and other cryptographic methods to protect confidential and sensitive information from unauthorized access and breaches

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

The Acceptable Use Policy (AUP) and the User Access Control Policy from the sample IT security policy framework definition mitigate risk in the User Domain. The AUP sets guidelines for acceptable behavior and use of IT resources by users, while the User Access Control Policy defines the processes for granting, modifying, and revoking user access to systems and data, ensuring that only authorized users have appropriate access rights

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

The Acceptable Use Policy (AUP) and the User Access Control Policy from the sample IT security policy framework definition mitigate risk in the User Domain. The AUP sets guidelines for acceptable behavior and use of IT resources by users, while the User Access Control Policy defines the processes for granting, modifying, and revoking user access to systems and data, ensuring that only authorized users have appropriate access rights

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

An IT security policy framework facilitates easier monitoring and enforcement throughout an organization by providing centralized guidance and standards, clarifying roles and responsibilities for compliance, establishing standardized procedures for enforcement, allowing for regular updates to address evolving threats, supporting training and awareness initiatives, and enabling integration with security monitoring systems for automated compliance checks

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?

The policy definition that requires an organization to list its mission-critical business operations and functions, along with the accompanying IT systems, applications, and databases that support them, is typically found within a Business Continuity and Disaster Recovery Policy. This policy outlines procedures for identifying and prioritizing critical business functions and their dependencies on IT systems to ensure continuity in case of disruptions or disasters

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

It is common to find a Business Continuity Plan (BCP) Policy Definition and a Computer Security Incident Response Team (CSIRT) Policy Definition because they serve complementary yet distinct purposes in organizational security and resilience. The BCP Policy Definition ensures that an organization has plans in place to maintain essential business functions during and after a disaster or disruption, minimizing downtime and ensuring continuity. On the other hand, the CSIRT Policy Definition outlines procedures and responsibilities for responding to and managing security incidents promptly and effectively, protecting the organization's systems and data from threats. Together, these policies help organizations prepare for and respond to both operational disruptions and security incidents comprehensively

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 typically includes guidelines on how data should be classified based on its sensitivity and importance. Part of this classification often includes requirements for encryption based on the sensitivity level of the data. Therefore, the Data Classification Standard will define whether or not encryption is necessary for data while it resides in a database

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.

True. Your upstream Internet Service Provider (ISP) plays a critical role in your Denial of Service (DoS) / Distributed Denial of Service (DDoS) risk mitigation strategy at the LAN-to-WAN Domain's Internet ingress/egress point. Including the ISP in your strategy ensures coordination for filtering and mitigating DoS/DDoS attacks before they reach your network. This is typically addressed in a policy definition for Internet ingress/egress availability, outlining measures and responsibilities for ensuring continuous availability and protection against such attacks