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: _____

Student Name: _____

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

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

Lab #9 – Assessment Worksheet

Part B – Sample IT Security Policy Framework Definition

Course Name: _____

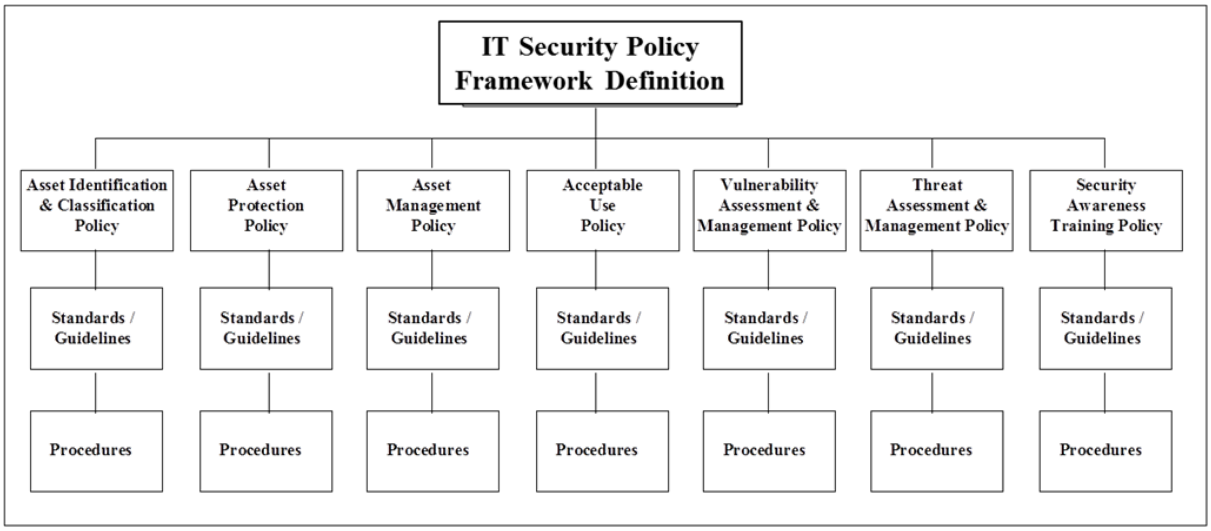
Student Name: _____

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

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

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: _____

Student Name: _____

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?

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

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?

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

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

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

7. Which policy definition helps achieve availability goals 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?

9. Which policy definitions from the sample IT security policy framework definition mitigate 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?

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

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?

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

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