Hands-On Steps

▶Note:
This is a paper-based lab. To successfully complete the deliverables for this lab, you will need access to Microsoft® Word or another compatible word processor. For some labs, you may also need access to a graphics line drawing application, such as Visio or PowerPoint. Refer to the Preface of this manual for information on creating the lab deliverable files.

1. On your local computer, **create the lab deliverable files**.
2. **Review the Lab Assessment Worksheet**. You will find answers to these questions as you proceed through the lab steps.
3. **Review** the seven domains of a typical IT infrastructure (see Figure 1).

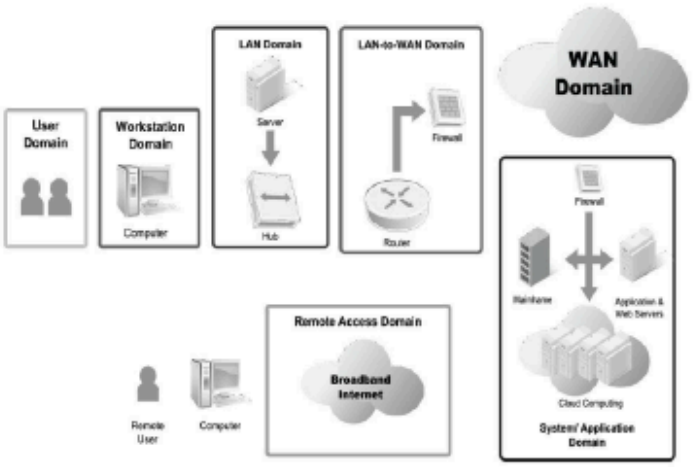

Figure 1 Seven domains of a typical IT infrastructure

4. In your Lab Report file, **describe** how risk can impact each of the seven domains of a typical IT infrastructure: User, Workstation, Local Area Network (LAN), Local Area Network-to-Wide Area Network (LAN-to-WAN), Wide Area Network (WAN), Remote Access, and System/Application domains.
5. **Review** the left-hand column of the following table of risks, threats, and vulnerabilities that were found in a health care IT infrastructure servicing patients with life-threatening conditions:

Risks, Threats, and Vulnerabilities	Primary Domain Impacted
Unauthorized access from public Internet	
Hacker penetrates IT infrastructure through modem bank	
Communication circuit outages	
Workstation operating system (OS) has a known software vulnerability	
Denial of service attack on organization's e-mail server	
Remote communications from home office	
Workstation browser has software vulnerability	
Weak ingress/egress traffic-filtering degrades performance	
Wireless Local Area Network (WLAN) access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	
Doctor destroys data in application, deletes all files, and gains access to internal network	
Fire destroys primary data center	
Intraoffice employee romance gone bad	
Loss of production data server	
Unauthorized access to organization-owned workstations	
LAN server OS has a known software vulnerability	
Nurse downloads an unknown e-mail attachment	
Service provider has a major network outage	
A technician inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers	
Virtual Private Network (VPN) tunneling between the remote computer and ingress/egress router	

▶Note:

Some risks will affect multiple IT domains. In fact, in real-world environments, risks and their direct consequences will most likely span across several domains. This is a big reason to implement controls in more than one domain to mitigate those risks. However, for the exercise in step 6 that follows, consider and select only the domain that would be most affected.

Subsequent next steps in the real world include selecting, implementing, and testing controls to minimize or eliminate those risks. Remember that a risk can be responded to in one of four ways: accept it, treat it (minimize it), avoid it, or transfer it (for example, outsource or insurance).

6. In your Lab Report file, **complete** the table from the previous step by identifying which of the seven domains of a typical IT infrastructure will be most impacted by each item in the table's left-hand column and **explain** why.

▶Note:
This completes the lab. **Close** the **Web browser**, if you have not already done so.

Evaluation Criteria and Rubrics

The following are the evaluation criteria for this lab that students must perform:

1. Identify common risks, threats, and vulnerabilities found throughout the seven domains of a typical IT infrastructure. – **[25%]**
2. Align risks, threats, and vulnerabilities to one of the seven domains of a typical IT infrastructure. – **[25%]**
3. Given a scenario, prioritize risks, threats, and vulnerabilities based on their risk impact to the organization from a risk-assessment perspective. – **[25%]**
4. Prioritize the identified critical, major, and minor risks, threats, and software vulnerabilities found throughout the seven domains of a typical IT infrastructure. – **[25%]**

Lab #1 - Assessment Worksheet

Identifying Threats and Vulnerabilities in an IT Infrastructure

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you identified known risks, threats, and vulnerabilities, and you organized them. Finally, you mapped these risks to the domain that was impacted from a risk management perspective.

Lab Assessment Questions & Answers

1. Health care organizations must strictly comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules that require organizations to have proper security controls for handling personal information referred to as "protected health information," or PHI. This includes security controls for the IT infrastructure handling PHI. Which of the listed risks, threats, or vulnerabilities can violate HIPAA privacy and security requirements? List one and justify your answer in one or two sentences.

2. How many threats and vulnerabilities did you find that impacted risk in each of the seven domains of a typical IT infrastructure?

3. Which domain(s) had the greatest number of risks, threats, and vulnerabilities?

4. What is the risk impact or risk factor (critical, major, and minor) that you would qualitatively assign to the risks, threats, and vulnerabilities you identified for the LAN-to-WAN Domain for the health care and HIPAA compliance scenario?

5. Of the three System/Application Domain risks, threats, and vulnerabilities identified, which one requires a disaster recovery plan and business continuity plan to maintain continued operations during a catastrophic outage?

6. Which domain represents the greatest risk and uncertainty to an organization?

7. Which domain requires stringent access controls and encryption for connectivity to corporate resources from home?

8. Which domain requires annual security awareness training and employee background checks for sensitive positions to help mitigate risks from employee sabotage?

9. Which domains need software vulnerability assessments to mitigate risk from software vulnerabilities?

10. Which domain requires acceptable use policies (AUPs) to minimize unnecessary user-initiated Internet traffic and can be monitored and controlled by Web content filters?

11. In which domain do you implement Web content filters?

12. If you implement a Wireless LAN (WLAN) to support connectivity for laptops in the Workstation Domain, which domain does WLAN fall within?

13. Under the Gramm-Leach-Bliley-Act (GLBA), banks must protect customer privacy. A given bank has just implemented its online banking solution that allows customers to access their accounts and perform transactions via their computers or personal digital assistant (PDA) devices. Online banking servers and their public Internet hosting would fall within which domains of security responsibility?

14. True or false: Customers who conduct online banking on their laptops or personal computers must use Hypertext Transfer Protocol Secure (HTTPS), the secure and encrypted version of Hypertext Transfer Protocol (HTTP) browser communications. HTTPS encrypts Web page data inputs and data through the public Internet and decrypts that Web page and data on the user's PC or device.

15. Explain how a layered security strategy throughout the seven domains of a typical IT infrastructure can help mitigate risk exposure for loss of privacy data or confidential data from the System/Application Domain.