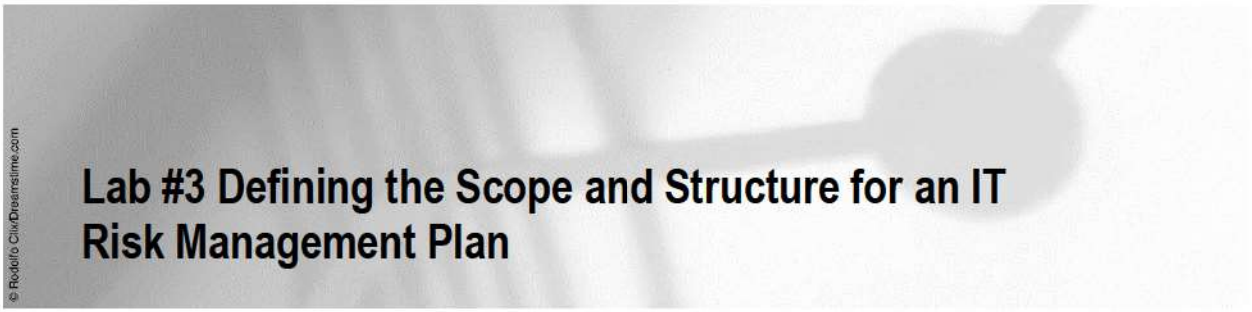

Lab #3 Defining the Scope and Structure for an IT Risk Management Plan

Introduction

Every company needs to take risks to thrive, but not too much risk which could be catastrophic. Finding the balanced amount of risk requires identifying what opportunities (or threats) are present, understanding how significant each of them is, recognizing what action to take to smartly handle both opportunities and risks, and lastly, monitoring all of the above, including discovering more prospects and threats. All told, this is called risk management. Specific to the seven domains of the IT infrastructure, this lab will cover IT risk management.

In this lab, you will define the purpose of an IT risk management plan, you will define the scope for an IT risk management plan that encompasses the seven domains of a typical IT infrastructure, you will relate the risks, threats, and vulnerabilities to the plan, and you will create an IT risk management plan outline that incorporates the five major parts of an IT risk management process.

Learning Objectives

Upon completing this lab, you will be able to:

- Define the purpose and objectives of an IT risk management plan.
- Define the scope and boundary for an IT risk management plan to encompass the seven domains of a typical IT infrastructure.
- Relate identified risks, threats, and vulnerabilities to an IT risk management plan and risk areas.
- Incorporate the five major parts of an IT risk management process into a risk management plan's outline.
- Craft an outline for an IT risk management plan, which includes the seven domains of a typical IT infrastructure and the five major parts of risk management and risk areas.

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file;
2. Lab Assessments file.

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. On your local computer, **open** a new **Internet browser window**.
4. Using your favorite search engine**, search for information** on the **IT risk management process**.
5. **Briefly review** at least five of the first page results.
6. In the address box of your Internet browser, **type** the URL **http://www.uvm.edu/~erm/RiskAssessmentGuide.pdf and press Enter to open the Web site**.
7. **Review** the PDF titled "Guide to Risk Assessment & Response."

▶Note:
Take special note of the University of Vermont's "Guide to Risk Assessment & Response" document and the insightful sections titled "Things to Keep in Mind" and "Steps to Follow" for each of the assessment steps.

8. In the address box of your Internet browser, **type** the URL **https://web.archive.org/web/20130418005540/http://www.education.nt.gov.au/__data/assets/pdf_file/0011/4106/risk_management_process.pdf and press Enter to open the Web site**.
9. **Review** the PowerPoint slide deck titled "The Risk Management Process."
10. In your Lab Report file, **describe** in what ways the risk management process in both IT and non-IT environments are similar. Briefly describe in your own words the five major steps of risk management: plan, identify, assess, respond, and monitor.
11. In your Lab Report file, **describe** the plan.
12. **Review** the seven domains of a typical IT infrastructure (see Figure 1).

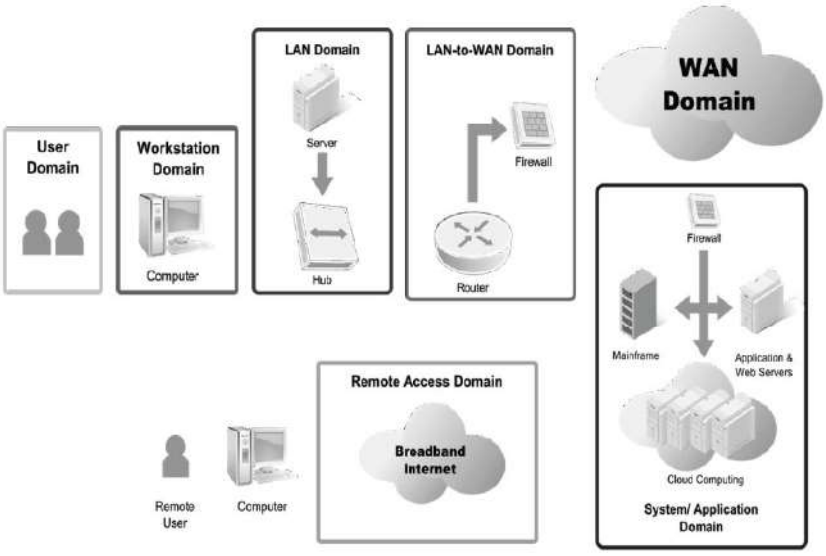

Figure 1 Seven domains of a typical IT infrastructure

13. Using the following table of risks, threats, and vulnerabilities that were found in a health care IT infrastructure servicing patients with life-threatening conditions, **review** the risks in the following table. **Consider** how you might manage each risk and which of the seven domains each one affects:

Risks, Threats, and Vulnerabilities
Unauthorized access from public Internet
Hacker penetrates IT infrastructure
Communication circuit outages
Workstations
Workstation operating system (OS) has a known software vulnerability
Denial of service attack on organization's e-mail
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 Local Area Network (LAN) connectivity within a warehouse
Need to prevent rogue users from unauthorized WLAN access
User 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
User downloads an unknown e-mail attachment
Service provider has a major network outage

User 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

14. In your Lab Report file, for each of the domains, **create** an outline in the scope of your risk management plan. Include the following topics—the five major parts of an IT risk management process—for each domain:

    - Risk planning
    - Risk identification
    - Risk assessment
    - Risk response
    - Risk monitoring

▶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. Define the purpose and objectives of an IT risk management plan. – **[20%]**
2. Define the scope and boundary for an IT risk management plan to encompass the seven domains of a typical IT infrastructure. – **[20%]**
3. Relate identified risks, threats, and vulnerabilities to an IT risk management plan and risk areas. – **[20%]**
4. Incorporate the five major parts of an IT risk management process into a risk management plan's outline. – **[20%]**
5. Craft an outline for an IT risk management plan, which includes the seven domains of a typical IT infrastructure and the five major parts of risk management and risk areas. – **[20%]**

Lab #3 - Assessment Worksheet

Defining the Scope and Structure for an IT Risk Management Plan

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you defined the purpose of an IT risk management plan, you defined the scope for an IT risk management plan that encompasses the seven domains of a typical IT infrastructure, you related the risks, threats, and vulnerabilities to the plan, and you created an IT risk management plan outline that incorporates the five major parts of an IT risk management process.

Lab Assessment Questions & Answers

1. What is the goal or objective of an IT risk management plan?

2. What are the five fundamental components of an IT risk management plan?

3. Define what risk planning is.

4. What is the first step in performing risk management?

5. What is the exercise called when you are trying to gauge how significant a risk is?

6. What practice helps address a risk?

7. What ongoing practice helps track risk in real time?

8. True or False: Once a company completes all risk management steps (identification, assessment, response, and monitoring), the task is done.

9. Given that an IT risk management plan can be large in scope, why is it a good idea to develop a risk management plan team?

10. In the seven domains of a typical IT infrastructure, which domain is the most difficult to plan, identify, assess, treat, and monitor?

11. Which compliance laws or standards does the health care organization mentioned in the Hands-On Steps have to comply with (consider these: Health Insurance Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley Act [GLBA], and Family Educational Rights and Privacy Act [FERPA])? How does this impact the scope and boundary of its IT risk management plan?

12. How did the risk identification and risk assessment of the identified risks, threats, and vulnerabilities contribute to your IT risk management plan outline?

13. What risks, threats, and vulnerabilities did you identify and assess that require immediate risk mitigation given the criticality of the threat or vulnerability?

14. For risk monitoring, what are some techniques or tools you can implement in each of the seven domains of a typical IT infrastructure to help mitigate risk?

15. For risk mitigation, what processes and procedures can help streamline and implement risk-mitigation solutions to the production IT infrastructure?

16. What is the purpose of a risk register?

17. How does risk response impact change control management and vulnerability management?