# Lab Name: Lab#6 Developing a Risk-Mitigation Plan Outline for an IT Infrastructure

# 

University of the Cumberlands

Dr. Richmond Ibe

Jacob Jeffers

ISOL 533 – Info Security and Risk Management

4/7/2021

Table of Contents

Cover Page ……………………………………………………………………………………….1

Table of Contents …………………………………………………………………………………2

Lab Deliverables ………………………………………………………………………………….3

Conclusion ………………………………………………………………………………………..9

References ……………………………………………………………………………………….10

Lab Deliverables

**Introduction**

Identifying and assessing risks is challenging, but treating them is another matter entirely. Treating risks means making changes based on a risk assessment and probably a few hard decisions. When treating even the most straightforward of risks, practice due diligence by documenting what steps you are taking to mitigate the risk. If you don’t document the change and the reasoning behind it, it’s possible that your organization could reverse the mitigation and reintroduce the risk based on the notion of “but that’s how we always did it before.”

After you’ve addressed a risk, appoint someone to make certain that the risk treatment is being regularly applied. If a security incident arises even with the change in place, having a single person in charge will ensure that any corrective action aligns with the risk-mitigation plan. You’re not appointing someone so you can blame that person if things go wrong; you are instead investing that individual with the autonomy to manage the incident effectively. The purpose of a risk-mitigation plan is to define and document procedures and processes to establish a baseline for ongoing mitigation of risks in the seven domains of an IT infrastructure.

In this lab, you will identify the scope for an IT risk-mitigation plan, you will align the plan’s major parts with the seven domains of an IT infrastructure, you will define the risk-mitigation steps, you will define procedures and processes needed to maintain a security baseline for ongoing mitigation, and you will create an outline for an IT risk-mitigation plan.

**Lab Objectives**

Upon completing this lab, you will be able to:

1. Identify the scope for an IT risk-mitigation plan focusing on the seven domains of a typical IT infrastructure.
2. Align the major parts of an IT risk-mitigation plan in each of the seven domains of a typical IT infrastructure.
3. Define the tactical risk-mitigation steps needed to remediate the identified risks, threats, and vulnerabilities commonly found in the seven domains of a typical IT infrastructure.
4. Define procedures and processes needed to maintain a security baseline definition for ongoing risk mitigation in the seven domains of a typical IT infrastructure.
5. Create an outline for an IT risk-mitigation plan encompassing the seven domains of a typical IT infrastructure.

**Hands-On Steps**

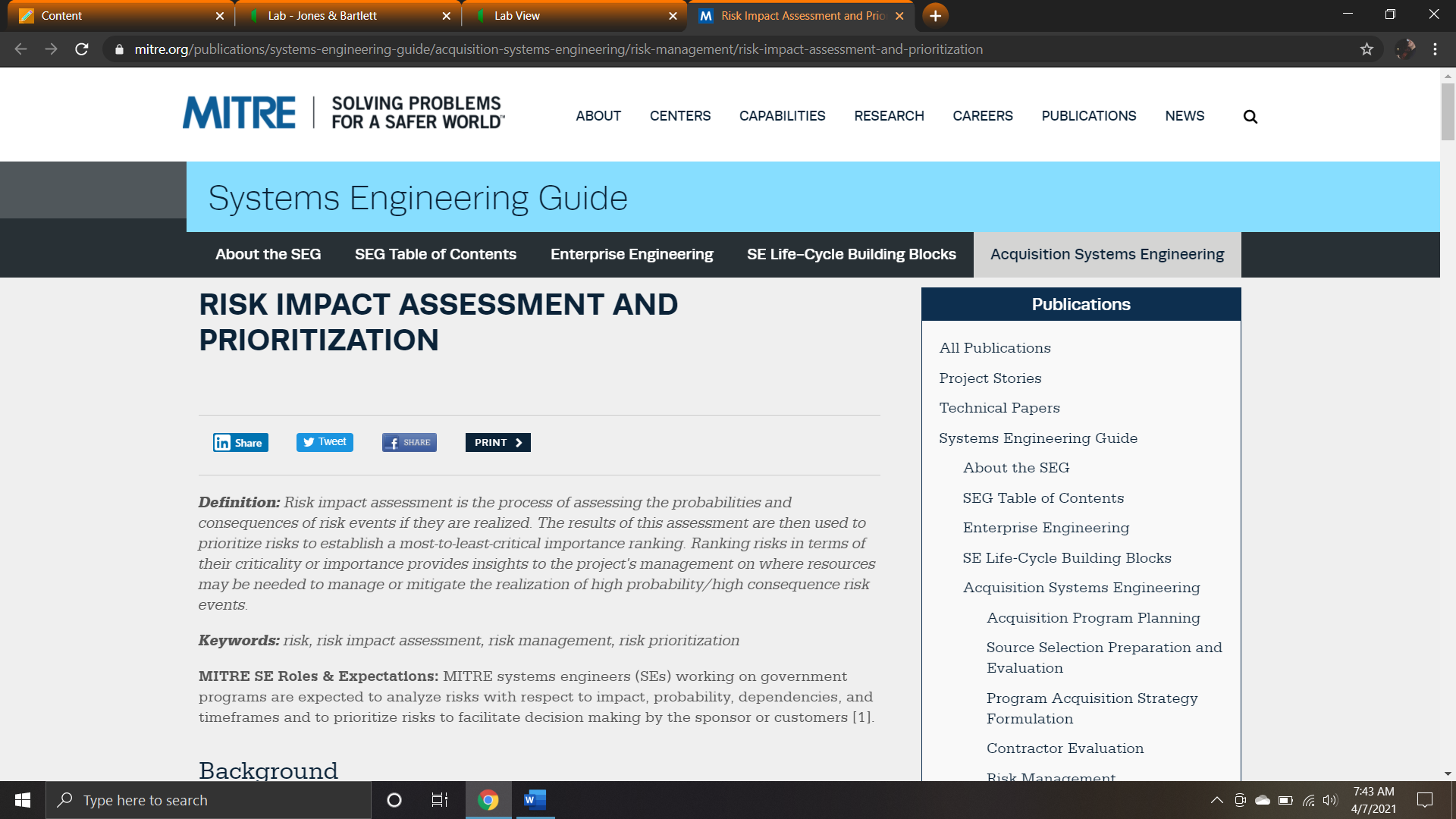
Step 1: This document will serve as the lab report.

Step 2: The seven domains of a typical IT infrastructure are the user, LAN, LAN to WAN, WAN, workstation, remote access, and systems/application.

Step 3:

|  |  |  |
| --- | --- | --- |
| **Risks, Threats, and Vulnerabilities** | **Primary Domain Impacted** | **Risk Impact/ Factor** |
| Unauthorized access from public Internet | LAN-to-WAN | 1 |
| User destroys data in application and deletes all files | User | 2 |
| Hacker penetrates your IT infrastructure and gains access to your internal network | System/Application | 1 |
| Intraoffice employee romance gone bad | User | 3 |
| Fire destroys primary data center | LAN | 1 |
| Service provider service level agreement (SLA) is not achieved | LAN -to- WAN | 1 |
| Workstation operating system (OS) has a known software vulnerability | LAN -to- WAN | 3 |
| Unauthorized access to organization-owned workstations | User | 2 |
| Loss of production data | System/Application | 2 |
| Denial of service attack on organization Demilitarized Zone (DMZ) and e-mail server | LAN -to- WAN | 2 |
| Remote communications from home office | Remote Access | 2 |
| Local Area Network (LAN) server OS has a known software vulnerability | LAN | 3 |
| User downloads and clicks on an unknown e-mail attachment | User | 2 |
| Workstation browser has a software vulnerability | Workstation | 3 |
| Mobile employee needs secure browser access to sales-order entry system | Remote Access | 1 |
| Service provider has a major network outage | WAN | 3 |
| Weak ingress/egress traffic-filtering degrades performance | LAN -to- WAN | 2 |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers | User | 1 |
| Virtual Private Network (VPN) tunneling between remote computer and ingress/egress router is needed | Remote Access | 1 |
| Wireless Local Area Network (WLAN) access points are needed for LAN connectivity within a warehouse | LAN -to- WAN | 2 |
| Need to prevent eavesdropping on WLAN due to customer privacy data access | WAN | 1 |
| Denial of service (DoS)/distributed denial of service (DDoS) attack from the Wide Area Network (WAN)/Internet | WAN | 1 |

Step 4: I have reviewed the executive summary from the lab manual, and I have organized the risk impact column.

Step 5: I have navigated to the web browser.

Step 6: I have read the article.

Step 7: The purpose of organizing this information allows the organization to quantify the amount of money that a potential risk might have.

Step 8:

Prioritization of identified risks, threats, and vulnerabilities organized into the seven domains

Critical “1” risks, threats, and vulnerabilities identified throughout the IT infrastructure

Implementation plans for remediation

Short-term remediation steps for critical “1” risks, threats, and vulnerabilities

Long-term remediation steps for major “2” and minor “3” risks, threats, and vulnerabilities

Cost magnitude estimates for work effort and security solutions

Executive Summary

Step 9:

A risk-mitigation plan starts with prioritizing risks, threats, and vulnerabilities. Then it consists of labeling them according to their risk factor. Remediation plans will then be set in front of the organization – both short-term and long-term. The cost estimates for this will be shown, and it will be presented in a summary.

Conclusion

In this lab, I have identified the scope for an IT risk-mitigation plan, aligned the plan’s major parts with the seven domains of an IT infrastructure, defined the risk-mitigation steps and procedures and processes needed to maintain a security baseline for ongoing mitigation, and created an outline for an IT risk-mitigation plan.

References

Gibson, D. (2014). Managing Risk in Information Systems (2nd ed.). Jones & Bartlett Learning.