Assessment Worksheet

Developing a Risk-Mitigation Plan Outline for an IT Infrastructure

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

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

Lab Assessment Questions & Answers

1. Why is it important to prioritize your IT infrastructure risks, threats, and vulnerabilities?

2. Based on your executive summary produced in the Performing a Qualitative Risk Assessment for an IT Infrastructure lab in this lab manual, what is the primary focus of your message to executive management?

3. Given the scenario for your IT risk-mitigation plan, what influence did your scenario have on prioritizing your identified risks, threats, and vulnerabilities?

4. What risk-mitigation solutions do you recommend for handling the following risk element: User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers?

5. What is a security baseline definition?

6. What questions do you have for executive management to finalize your IT risk-mitigation plan?

7. What is the most important risk-mitigation requirement you uncovered and want to communicate to executive management? In your opinion, why is this the most important risk-mitigation requirement?

8. Based on your IT risk-mitigation plan, what is the difference between short-term and long-term risk-mitigation tasks and ongoing duties?

9. For which of the seven domains of a typical IT infrastructure is it easy to implement risk-mitigation solutions but difficult to monitor and track effectiveness?

10. Which of the seven domains of a typical IT infrastructure usually contains privacy data in systems, servers, and databases?

11. Which of the seven domains of a typical IT infrastructure can access privacy data and also store it on local hard drives and disks?

12. Why is the Remote Access Domain the most risk-prone of all in a typical IT infrastructure?

13. When considering the implementation of software updates, software patches, and software fixes, why must you test the upgrade or software patch before you implement it as a risk-mitigation tactic?

14. Are risk-mitigation policies, standards, procedures, and guidelines needed as part of your long-term risk-mitigation plan? Why or why not?

15. If an organization under a compliance law is not in compliance, how critical is it for your organization to mitigate this noncompliance risk element?