Lab #3: Assessment Worksheet

Define the Scope & Structure for an IT Risk Management Plan

Course Name: IAM302

Student Name: Huynh Ngoc Quang

Instructor Name: Mr. Mai Hoang Dinh

Lab Due Date: September 21, 2024

Overview

The Instructor will assign your group one of the following scenarios and industry verticals. You must align your IT risk management plan from this scenario and industry vertical perspective along with any compliance law requirements.

1. Circle the scenario and industry vertical your Instructor assigned to your group:
    a. **Healthcare provider under HIPPA compliance law**
    b. Regional bank under GLBA compliance law
    c. Nationwide retailer under PCI DSS standard requirements
    d. Higher-education institution under FERPA compliance law
2. Make sure your table of contents addresses your scenario and vertical industry.
3. Make sure your table of contents includes at a minimum, the five major parts of IT risk management:
    - Risk planning
    - Risk identification
    - Risk assessment
    - Risk mitigation
    - Risk monitoring
4. Make sure your table of contents is executive management ready and addresses all the risk topics and issues needed for executive management awareness.
5. Answer Lab #3 – Assessment Worksheet questions and submit as part of your Lab #3 deliverables

Lab #3: Assessment Worksheet

Define the Scope & Structure for an IT Risk Management Plan

Overview

Answer the following Lab #3 – Assessment Worksheet questions pertaining to your IT risk management plan design and table of contents

Lab Assessment Questions:

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

   The goal is to create a risk management plan for a healthcare provider, focusing on compliance with the Health Insurance Portability and Accountability Act (HIPAA). This plan will protect sensitive patient data and ensure that all IT infrastructure meets regulatory requirements.

2. What are the five fundamental components of an IT risk management plan?
   - **Risk Planning**: Planning involves establishing a clear risk management policy, ensuring HIPAA compliance, and assigning roles and responsibilities for risk oversight.
   - **Risk Identification**: Identify potential risks such as data breaches, insider threats, and misconfigurations of healthcare IT systems. This includes risks associated with electronic protected health information (ePHI).
   - **Risk Assessment**: Conduct an evaluation of the identified risks, determining their impact and likelihood. Assess threats to ePHI, network security, and user access control systems.
   - **Risk Mitigation**: Develop strategies to reduce risks, such as implementing encryption, regular audits, and staff training to ensure compliance with HIPAA.
   - **Risk Monitoring**: Establish a system for continuous monitoring of risks. This could include automated threat detection tools, periodic audits, and incident response plans.
3. Define what risk planning is.
4. What is the first step in performing risk management?

   First Step in Risk Management: Risk identification is the first step, where potential vulnerabilities and threats are discovered.

5. What is the exercise called when you are trying to identify an organization's risk health?

   Risk assessment, where the organization's current risk profile is evaluated.
6. What practice helps reduce or eliminate risk?

Risk mitigation strategies, such as encryption and access control, help to reduce or eliminate risk.

7. What on-going practice helps track risk in real-time?
   Risk monitoring, such as using real-time alert systems and regular audits, tracks risks continuously.
8. Given that an IT risk management plan can be large in scope, why is it a good idea to development a risk management plan team?
   It's a good idea to have a team due to the complexity of managing risk across different areas of IT and to ensure effective decision-making.
9. Within the seven domains of a typical IT infrastructure, which domain is the most difficult to plan, identify, assess, remediate, and monitor?
   The user domain is often the most difficult due to human errors, insider threats, and complex access management.
10. From your scenario perspective, with which compliance law or standard does your organization have to comply? How did this impact the scope and boundary of your IT risk management plan?
    HIPAA compliance expands the scope to cover all aspects of patient data security, from data transmission to storage and user access.
11. How did the risk identification and risk assessment of the identified risks, threats, and vulnerabilities contribute to your IT risk management plan table of contents?
    Identifying risks related to HIPAA compliance, such as unauthorized access to patient data, will shape the content of the risk management plan, ensuring a focus on protecting sensitive health information.
12. What risks, threats, and vulnerabilities did you identify and assess that require immediate risk mitigation given the criticality of the threat or vulnerability?
    Immediate risks include data breaches and unauthorized access to ePHI, which could result in severe penalties and loss of patient trust.
13. For risk monitoring, what techniques or tools can you implement within each of the seven domains of a typical IT infrastructure to help mitigate risk?
    Use intrusion detection systems (IDS), data encryption, and access control systems to monitor risks in real-time.
14. For risk mitigation, what processes and procedures are needed to help streamline and implement risk mitigation solutions to the production IT infrastructure?
    Implement robust access controls, regular audits, and staff training programs to ensure risks are properly mitigated.
15. How does risk mitigation impact change control management and vulnerability management?

Risk mitigation must be integrated with change control processes to ensure that any changes to the IT environment are evaluated for new risks. Vulnerability management involves regular patching and updates to reduce the attack surface.