Lab #3: Assessment Worksheet
Define the Scope & Structure for an IT Risk Management Plan

Course Name: IAA202
Student Name: Dang Hoang Nguyen
Lab Due Date: June, 02 2023

Overview

You must align your IT risk management plan from this scenario and industry vertical perspective along with any compliance law requirements.

1. Scenario and industry vertical given: Healthcare provider under HIPPA 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 Assessment Questions

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

   The goal of an IT risk management plan is to minimize potential threats that could harm an organization's information technology systems and infrastructure by identifying, assessing, and prioritizing risks and developing a strategy to manage them.

2. What are the five fundamental components of an IT risk management plan?
   - Risk planning
   - Risk identification
   - Risk assessment
   - Risk mitigation
   - Risk monitoring

3. Define what risk planning is.

   Risk planning is a way to identifying the risks that could be potentially harm to the business, project, etc. It involves in analyzing the impact, mitigation, determine the best course of action to manage them. It is a process throughout the life cycle of the project, and it will have us to completed the project on time, within budget and with minimal disruption from unforeseen events.

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

   Risk identification

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

   Risk assessment

6. What practice helps reduce or eliminate risk?

   Risk mitigation

7. What on-going practice helps track risk in real-time?

   Risk monitoring

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?

   When developing a risk management plan team, risk can be identified assessed, and managed in a structured and systematic way. A team with a lot of people will bring many perspectives as well as the expertise to solve the problem.

Having a team for IT risk management will quickly identify the risk and threat during the life cycle of the product. The team can work proactively to identify potential risks and develop mitigation strategies that help minimize their impact on the organization's objectives.

9. Within the seven domains of a typical IT infrastructure, which domain is the most difficult to plan, identify, assess, remediate, and monitor?

   System / Application domain, because it contains all infrastructure of the system such as operating system (OS), hardware system, etc. That make up the IT infrastructure, which can be diverse and constantly changing

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?

    For the scenario of healthcare provider under HIPPA compliance law, our organization must comply with those strict regulations for the data, security and privacy of the patient by the PHI, which mean that the IT systems and processes involved in handling PHI must be designed, implemented, and maintained to meet HIPAA's requirements.

    We must make sure that all the potential risks to PHI are all identified and having some appropriate solutions such that data encryption using some tough encryption such as RSA, AES, etc. Also having some other solution like access controls, recovery processes. Also, we have to scan and identify the risks frequently in order not to turning into trouble. And don't put too many eggs into one bowl.

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?

    Risk identification and risk assessment is two important phases to contribute to the risk management plan table of contents. Risk identification help us to identify all the potential risks that could impact to the CIA of PHI. After these risks are identified, then the risk assessment will do the next part, this process helps to determine the likelihood and potential impact of each risk on the organization and its information systems. Through this analysis, organizations can prioritize which risks pose the greatest threat and require immediate attention.

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

    - Unauthorize access to PHI data
    - Attack like such as phishing, sending malwares, ransomware create a backdoor for hacker taking the privacy data

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?

    To help mitigate the risk, I supposed that, in some domain such that

    - user domain, which is the most dangerous one, we should implement strong password such that using some regular expression like the password must be 10 words, which having at upper- and lower-case letter, number, special character. Also, have two-factor authentication.
    - Workstation domain: maintain the computer regularly, always keep up-to-date with the latest patch, also update the anti-virus software daily
    - Lan-to-Wan: using firewall to capture all the traffic that go in and out, or using some IPS/IDS system
    - WAN domain: we can use VPNs to secure
    - System/Application domain: Vulnerability scanning and pentest as well, we must have a role-base control when accessing this domain, auditing and logging

14. For risk mitigation, what processes and procedures are needed to help streamline and implement risk mitigation solutions to the production IT infrastructure?

    To streamline and implement risk mitigation solutions in production IT infrastructure, processes and procedures such as risk assessment, vulnerability management, security testing, incident response planning, change management, and regular security audits are needed. These measures can help identify and prioritize potential risks, implement appropriate controls and safeguards, and continually monitor and improve the overall security posture of the production IT environment.

15. How does risk mitigation impact change control management and vulnerability management?

    Risk mitigation plays an important role in control management and vulnerability management. , risk mitigation helps to identify potential risks associated with proposed changes to the IT environment and implement appropriate controls to reduce the likelihood of adverse impacts on system availability, confidentiality, and integrity. In vulnerability management will identifying and prioritizing vulnerabilities based on their potential impact on the organization and implementing appropriate controls to reduce the associated risks.