Lab # 3 — Assessment Worksheet

**Course Name and Number: IAA202**

**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Mai Hoang Dinh**

## **Define the Scope & Structure for an IT Risk Management Plan**

***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.

|  |  |
| --- | --- |
| **Risk – Threat – Vulnerability** | **Policy Definition Required** |
| Unauthorized access from public Internet | Access Control Policy Definition |
| User destroys data in application and deletes all files | Acceptable Use Policy, Mandated Security Awareness Training Policy Definition |
| Hacker penetrates your IT infrastructure and gains access to your internal network | Vulnerability Management & Vulnerability Window Policy Definition |
| Intra-office employee romance gone bad | BIA Policy Definition |
| Fire destroys primary data center | Business Continuity & Disaster Recovery Policy Definition, Production Data Back-up Policy Definition |
| Communication circuit outages | Business Continuity & Disaster Recovery Policy Definition |
| Workstation OS has a known software vulnerability | Vulnerability Management & Vulnerability Window Policy Definition |
| Unauthorized access to organization owned Workstations | Access Control Policy Definition |
| Loss of production data | Production Data Back-up Policy Definition |
| Denial of service attack on organization e-mail Server | Vulnerability Management & Vulnerability Window Policy Definition |
| Remote communications from home office | Remote Access Policy Definition |
| LAN server OS has a known software vulnerability | Vulnerability Management & Vulnerability Window Policy Definition |
| User downloads an unknown e-mail attachment | Acceptable Use Policy, Mandated Security Awareness Training Policy Definition |
| Workstation browser has software vulnerability | Vulnerability Management & Vulnerability Window Policy Definition |
| Service provider has a major network outage | WAN Service Availability Policy Definition |
| Weak ingress/egress traffic filtering degrades | Performance Internet Ingress/Egress Traffic Policy Definition |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | Acceptable Use Policy |
| VPN tunneling between remote computer and ingress/egress router | Remote Access Policy Definition, Internet Ingress/Egress Traffic Policy Definition |
| WLAN access points are needed for LAN connectivity within a warehouse | Access Control Policy Definition |
| Need to prevent rogue users from unauthorized WLAN access | Data Classification Standard & Encryption Policy Definition |

***Lab Assessment Questions & Answers***

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

The goal or objective of an IT risk management plan is to identify hazards, assess the risks, control the risks and to monitor or review control measures. The IT risk management plan defines how risks are managed and controlled for all projects.

The goal of an IT risk management plan is to identify potential problems before they occur and have a plan for addressing them. IT Risk management looks at internal and external risks that could negatively impact a project. It plans how to manage and control the security of the project.

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

The five fundamental components of an IT risk management plan are as follows: Risk Planning, Risk Identification, Risk Assessment, Risk Response and Risk Monitoring.

1. **Define what risk planning is.**

Risk planning is to be prepared to foreseen risks, identify the risks and to develop and document the actions, strategies and methods to reduce the risk.

1. **What is the first step in performing risk management?**

The first step in performing risk management is to establish the context for risk assessment to set the stage for risk identification.

1. **What is the exercise called when you are trying to identify an organization’s risk health?**

Audit

1. **What practice helps reduce or eliminate risk?**

Risk Mitigation Steps

1. **What ongoing practice helps track risk in real time?**

Monitoring

1. **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?**

It is always beneficial to have a risk management plan team to continuously protect the organization from risks and threats. The team could share the responsibilities and work effectively in fulfilling their responsibilities. The employees come up with different plans and ways to mitigate the risks and thereby benefit the organization.

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

LAN-WAN

1. **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?**

Healthcare organization has to comply with HIPAA act because HIPAA deals with the health information of numerous people and being a healthcare organization, they would have all the health related and insurance related data and it is their responsibility to protect that data from any risk, threat and vulnerability. This impacts the boundary of IT risk management plan to develop a proper and effective risk management control in protecting the confidential information of health insurance and health information of the people.

1. **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 identifies all types of risks and risk assessment is useful in assessing the consequences and frequency of exposure to a hazard. IT management plan outline includes everything from establishing the objectives to reporting of risks of which the risk identification and assessment plays important role in preventing them from attacking the organizations and thereby causing loss of data, property and reputation.

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

Unauthorized access from public internet, User destroys data in application, deletes all files, and gains access to internal network and hacker penetrates IT infrastructure requires immediate risk mitigation.

1. **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?**

Different ways could be followed to mitigate risk in different domains. Having strong procedures and spreading awareness for User domain, strong firewalls and antivirus for workstation domain, port security for LAN domain, strong firewall to server for LAN-WAN domain, VPN client system and encryption for remote access, DMZ for Wan and data backups and servers for System/Application domain are effective. Overall, any kind of identification and steps taken to reduce the risks should help in mitigating risk.

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

Developing strict schedules with stringent controls, having IT audits and ensuring timely completion of tasks with proper remediation and reporting can lead to production IT infrastructure.

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

Change control is a continuous process for an organization and risk response step decides the best way to treat a risk, modify the risk and implement the plan so that the change control process is not disturbed. Risk response is used in assessing the response, determining the level of risk and developing the response. Vulnerability management is also well maintained as risk response reduces the risks and decreases the vulnerability of an organization getting affected by risks.