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

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 1/2/2023

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:
- 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.

Table of Contents

- **WHAT ARE THE DIFFERENT TYPES OF RISK?**

3. RISK ASSESSMENT
- **WHAT IS RISK ASSESSMENT?**
- **WHAT IS RISK ASSESSMENT LIKE?**
- **WHAT IS THE PURPOSE OF RISK ASSESSMENT?**

4. RISK MITIGATION
- **WHAT IS RISK MITIGATION?**
- **WHAT IS RISK MITIGATION LIKE?**
- **WHAT IS THE PURPOSE OF RISK MITIGATION?**

5. RISK MONITORING
- **WHAT IS RISK MONITORING?**
- **WHAT IS RISK MONITORING LIKE?**
- **WHAT IS THE PURPOSE OF RISK MONITORING?**

Lab Assessment Questions

1. What is the goal or objective of an IT risk management plan?
- The motive of the risk management Plan is to define how risks might be controlled, monitored and managed for the duration of the project.

2. What are the five fundamental components of an IT risk management plan?
-The components of a Risk Management Plan are: Risk Identification, Risk Analysis, Risk Evaluation, Risk Monitoring and Review.

3. Define what risk planning is.
- Risk planning is developing and documenting organized, comprehensive, and interactive strategies and methods for identifying risks.

4. What is the first step in performing risk management?
- One of the most important first steps for a risk management plan is to establish the objectives.

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

6. What practice helps reduce or eliminate risk?
- Risk Management.

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

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?
-Scope identifies obstacles. So, if the plan is that huge in scope, a team would paintings obviously collectively and not against to maintain its structure in nature and have consensus.

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

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?
- Honoring that the regulation calls for a pupil to get hold of grades from teachers bodily compliance.

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?
- It was detailed properly to locate provided information needed.

12. What risks, threats, and vulnerabilities did you identify and assess that require immediate risk mitigation given the criticality of the threat or vulnerability?
- Amongst different things, college and/or students weak or being situation to falling brief to economic, pleasure or every other immoral selfish advantage.

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?
- Some thing viable, guy or guy-made to correctly examine, pick out and deal with feasible risks.

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

- Control, remediation, assess and reporting are key.

15. How does risk mitigation impact change control management and vulnerability management?
- Alternate control is a systematic way to imminent exchange, inside an organization, it can save you the possibility of services turning into interrupted and if so, offer a plan to deliver them again up as quickly as feasible