## Lab #6: Assessment Worksheet

**Develop a Risk Mitigation Plan Outline for an IT Infrastructure**

**Course Name: IAA202**

**Student Name: Phan Tuan Minh**

**Lab Due Date:**

**Overview**

After completing your IT risk mitigation plan outline, answer the following Lab #6 – Assessment

Worksheet questions. These questions are specific to the IT risk mitigation plan outline you crafted as

part of Lab #6 – Develop a Risk Mitigation Plan Outline for an IT Infrastructure.

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

* It is important to prioritize because you must be aware of what the risks, threats, and vulnerabilities there are to your infrastructure. You need this so that you know where the most attention needs to be focused on.

**2. Based on your executive summary produced in Lab #4 – Perform a Qualitative Risk Assessment for an IT Infrastructure, what was the primary focus of your message to executive management. Why?**

* Setting up security measures through various means includes the following:
* Forcing users to update password every X number of days : Avoiding employees forgetting their password and preventing IT infrastracture from being hacked.
* Educating the users : Raise employees' awareness of internal information security
* Firewalls - Anti-malware : The most basic measures to protect information of the organization company. Anti-malware or firewalls that need periodic maintenance and upgrades

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

**Example:** A company starts to use a remote working platform when being quarantined because of COVID-19

**Risk:** Employees leak the code of online meeting or workstations

|  |  |  |  |
| --- | --- | --- | --- |
| **Solution** | **Risk Impact/Factor** | **Cost** | **Impact** |
| Educating the employees | Major | Pending | Minimize the wrong actions of employees |
| Change Password Regularly | Major | None | Improve software security and user behavior |
| Establishment of IT incident response team | Critical | Pending | Respond as quickly as possible to any unexpected IT problems |
| Upgrade firewall and security software | Critical | ~25.000.000 VND  (Reference price) | Upgrade the basic security system |
| Penetration Test regularly | Critical | ~25.000.000 VND  (Reference price) | Upgrade the basic security system & Detect security flaws |
| Make a list of departments and separate meeting links for employees and departments to use | Major | None | Restrict access of employees |
| Division of working hours | Major | None | Avoid system overload |

**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. Why?**

* A good antivirus program and have all devices scanned as soon as they are plugged in : Apply for some special project which needs extended devices or memory, but that needs confirmation from leaders of company.
* Educate employees : Raise employees' awareness of internal information security
* Disable optical drives/USB ports : Prevent employees from using IT infrasture for personal purpose and being leaked to be used for crime purpose