## Lab #10: Assessment Worksheet

**Create a CIRT Response Plan for a Typical IT Infrastructure**

**Course Name: IAA202**

**Student Name: Phan Tuấn Minh**

**Lab Due Date:**

**1. What risk mitigation security controls or security countermeasures do you recommend for the portion of the network that you built a CIRT response plan? Explain your answer.**

* Keep up-to-date systems as certain fixes and upgrades have protection to avoid bugs and vulnerabilities causing vulnerabilities to protection. Enable firewalls, as firewalls filter traffic to prevent unwanted traffic from entering vulnerable systems

**2. How does a CIRT plan help an organization mitigate risk?**

* It helps prepare an organization for accidents. When prepared, the company is able to respond much quicker and with concentrated action to the incidents

**3. How does a CIRT response plan help mitigate risk?**

* To respond to the incidents as fast as possible and with focused actions & preventions

**4. How does the CIRT post-mortem review help mitigate risk?**

* A post-mortem report will provide a full summary of the incident and the management of the response and program setup, safety countermeasures, guidelines for implementation to prevent the accident or violation from happening again

**5. Put the following in the proper sequence:**

Identification : 2

Containment : 3

Post-Mortem Review : 6

Eradication : 4

Preparation : 1

Recovery : 5