Lab # 10 — Assessment Worksheet

**Course Name and Number: IAA202**

**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Mai Hoang Dinh**

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

***Overview***

The best risk mitigation strategy requires building and implementing a CIRT response plan. This means you are preparing for potential computer/security incidents and practicing how to handle these incidents. Like any kind of remediation, the more you can plan, prepare, and practice, the more prepared you are to handle any risk situation. This lab presented how to apply the computer/security incident response methodology to handling incidents specific to a portion of the network infrastructure.

***Lab Assessment Questions & Answers***

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 systems up to date because some patches and updates have security to stop bug sand weaknesses from causing security vulnerabilities. Permit firewalls because firewalls will screen traffic to ensure that unwelcome traffic does not reach vulnerable systems.

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

It helps an organization prepare for incidents.

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

It helps to respond to incidents much quicker and with focused action. Provides appropriate and consistent response to such incidents

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

IT includes an after action review. The incident is examined along with the response to determine if there are any lessons to be leaned. The goals are to determine if the response was as effective as possible, and if the response can be improved.

1. **Why is it a good idea to have a protocol analyzer as one of your incident response tools when examining IP LAN network performance or connectivity issues?**

The protocol analyzer would need to investigate and analyze events to determine if they are actual incidents, or false positives.

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

Identification: 2

Containment: 3

Post-Mortem Review: 6

Eradication: 4

Preparation: 1

Recovery: 5

1. **Which step in the CIRT response methodology relates back to RTO for critical IT systems?**

Recovery

1. **Which step in the CIRT response methodology requires proper handling of digital evidence?**

Containment

1. **Which step in the CIRT response methodology requires review with executive management?**

Post-mortem review

1. **Which step in the CIRT response methodology requires security applications and tools readiness?**

Preparation