**Lab #2: Assessment Worksheet**

**Align Risk, Threats, & Vulnerabilities to COBIT P09 Risk Management Controls**

**Course Name: IAA202**

**Instructor Name: Vu Hoang**

**Lab Due Date:**

**Overview**

Think of the COBIT framework as a giant checklist for what an IT or Risk Management auditors would do if they were going to audit how your organization approaches risk management for your IT infrastructure. COBIT P09 defines 6 control objectives for assessing and managing IT risk within four different focus areas.

The first lab task is to align your identified threats and vulnerabilities from Lab #1 – How to Identify Threats and Vulnerabilities in Your IT Infrastructure.

**Lab Assessment Questions**

1. From the identified threats & vulnerabilities from Lab #1 – (List At Least 3 and No More than 5, High/Medium/Low Nessus Risk Factor Definitions for Vulnerabilities)

A.Intra-office employee romance gone bad – LOW

B.User insets CDs and USB hard drives with personal photos, music, and videos on organization owned computers – MEDIUM

C.User downloads and unknown email attachment – HIGH

D.User destroys data in application and deletes all files – MEDIUM/HIGH

E.Service provider has a major network outage – LOW

2. For the above identified threats and vulnerabilities, which of the following COBIT P09 Risk Management control objectives are affected?  PO9.1 IT Risk Management Framework –

PO9.1 IT Risk Management Framework – A

PO9.2 Establishment of Risk Context – none

PO9.3 Event Identification – B

PO9.4 Risk Assessment – C

PO9.5 Risk Response – D

PO9.6 Maintenance and Monitoring of a Risk Action Plan – E

3. From the identified threats & vulnerabilities from Lab #1 – (List At Least 3 and No More than 5), specify whether the threat or vulnerability impacts confidentiality – integrity – availability:

a. intra-office employee romance gone bad

b. loss of production data

c. denial of service attack on organization e-mail server

4. For each of the threats and vulnerabilities from Lab #1 (List at Least 3 and No More than 5 (that you have remediated, what must you assess as part of your overall COBIT P09 risk management approach for your IT infrastructure?

Denial of service attack- close the ports and change the passwords

Loss of Production Data- Backup the data and restore the data from the most recent known safe point.

Unauthorized access Workstation- Implement a policy where employees have to adjust their passwords every sixty days and that they must set a screen lockout when they step away from their workstation.

5. For each of the threats and vulnerabilities from Lab #1 – (List at Least 3 and No More than 5) assess the risk impact or risk factor that it has on your organization in the following areas and explain how this risk can be mitigated and managed:

a. Threat or Vulnerability #1:

Information – threat

Applications – Threat

Infrastructure – Threat

People – None

b. Threat or Vulnerability #2:

Information – Threat

Applications – Threat

Infrastructure – Threat

People – Threat with someone job

c. Threat or Vulnerability #3:

o Information – threat

o Applications – Vulnerability

o Infrastructure – Vulnerability

o People – Threat

d. Threat or Vulnerability #4:

o Information – Vulnerability

o Applications – Vulnerability

o Infrastructure – Vulnerability

o People – none

e. Threat or Vulnerability #5:

o Information – Vulnerability

o Applications – Vulnerability

o Infrastructure – Vulnerability

o People – threat

6. True or False – COBIT P09 Risk Management controls objectives focus on assessment and management of IT risk. True

7. When it’s too secure, people will not use it, when it’s not secure enough people run the risk of losing information.

8. When assessing the risk impact a threat or vulnerability has on your “information” assets, why must

you align this assessment with your Data Classification Standard? How can a Data Classification

Standard help you assess the risk impact on your “information” assets?

We have to align it because it helps you classify the importance and use of information. It will help determine the level of risk factor it is if it was ever compromised

9. When assessing the risk impact a threat or vulnerability has on your “application” and

“infrastructure”, why must you align this assessment with both a server and application software

vulnerability assessment and remediation plan?

You must assign it because it is what a high level company stand should be, anything less is unacceptable.

10. When assessing the risk impact a threat or vulnerability has on your “people”, we are concerned

with users and employees within the User Domain as well as the IT security practitioners who must

implement the risk mitigation steps identified. How can you communicate to your end-user

community that a security threat or vulnerability has been identified for a production system or

application? How can you prioritize risk remediation tasks?

You can inform the EU by sending out e-mails or company memos that informs everybody what the security threat or vulnerability is and how to prevent it. You can also either hold a training class or set up some kind of step by step instruction or how to video to inform and give tips on how to prevent it.

11. What is the purpose of using the COBIT risk management framework and approach?

COBIT weaves together models and approaches used by different IT specialties. This allows used for a wide range of enterprise needs, including information security, regulatory compliance, risk management and financial processing.

12. What is the difference between effectiveness versus efficiency when assessing risk and risk

management?

There must be a balance between efficiency, getting a task done quickly, and efficiency, completing a task completely.

13. Which three of the seven focus areas pertaining to IT risk management are primary focus areas of risk assessment and risk management and directly relate to information systems security?

Workstation, remote station, and system application domains.

14. Why is it important to assess risk impact from four different perspectives as part of the COBIT P.09

Framework?

This framework, although suggestive, allows the consideration of the risk/threat potential, recurrence possibilities, mediation actions available, and future maintenance of the IT system.

15. What is the name of the organization who defined the COBIT P.09 Risk Management

Framework Definition?

It was written by the IT Governance Institute (ITGI) with the Information Systems Audit and Control Association (ISACA).