Lab # 2 — Assessment Worksheet

**Course Name and Number: IAA202**

**Student Name: Tran Thanh Tuan**

**Student Id: SE161095**

**Instructor Name: Mai Hoang Dinh**

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

***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 & Answers***

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)
   1. User inserts cds and usb hard drives with personal photos, music ... on organization ownedcomputers – MEDIUM
   2. Workstations OS has a known software vulnerability – LOW
   3. User destroys data in application and deletes all files – MEDIUM
   4. Denial of Service attack of organized e-mail server – HIGH
   5. Unauthorized access to organization owned Workstation – HIGH
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 – d
* PO9.2 Establishment of Risk Context – none
* PO9.3 Event Identification – b, c, d
* PO9.4 Risk Assessment – a, c, e
* PO9.5 Risk Response – none
* PO9.6 Maintenance and Monitoring of a Risk Action Plan – none

1. 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:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Confidentiality | Integrity | Availability |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. 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 of organized e-mail server
* User downloads and unknown email attachment
* Loss of Production
* DataWorkstation browser has software vulnerability
* Unauthorized access to organization owned Workstation

1. 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:
   1. Threat or Vulnerability #1: Denial of Service attack of organized e-mail server
      * Information –Threat
      * Applications –Threat
      * Infrastructure –Threat
      * People – None
   2. Threat and Vulnerability #2: Loss of Production Data
      * Information – Threat
      * Applications – Threat
      * Infrastructure – Threat
      * People – Threat to someone’s job
   3. Threat or Vulnerability #3: Unauthorized access to organization owned Workstation
      * Information – Threat
      * Application – Vulnerability
      * Infrastructure – Vulnerability
      * People – Threat
   4. Threat or Vulnerability #4: Workstation browser has software vulnerability
      * Information – Vulnerability
      * Application – Vulnerability
      * Infrastructure – Vulnerability
      * People – None
   5. Threat or Vulnerability #5: User downloads an unknown e-mail attachment
      * Information – Vulnerability
      * Application – Vulnerability
      * Infrastructure – Vulnerability
      * People – Threat
2. True or False – COBIT P09 Risk Management controls objectives focus on assessment and management of IT risk.

True.

1. Why is it important to address each identified threat or vulnerability from a C-I-A perspective?

Because CIA is a balanced perspective. When it’s too secure, people will not use it, when it’s not secure enough people run the risk of losing information.

1. 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 of the information and use. It will determine the level the risk factor is if it was compromised.

1. 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?

It is what any high level company works on. Anything less is unacceptable

1. 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?

Send e-mail, memos, setup a training class. The risk that can come to users the quickest or highest threatmust be prioritized first.

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

Comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise information and technology assets (IT). Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

1. What is the difference between effectiveness versus efficiency when assessing risk and risk management?

Effectiveness is following the instructions of a specific job while efficiency is doing the instructions in lesser time and cost. They say Effectiveness is doing what’s right and efficiency is doing things rightly done.

1. 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?

Assessing the risk, Mitigating Possible Risk and Monitoring the Result.

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

The more perspectives you have, the better view of all the risk that are available.

1. What is the name of the organization who defined the COBIT P.09 Risk Management Framework Definition?

The IT Governance Institute