## Lab #2: Assessment Worksheet

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

**Course Name: IAA202**

**Student Name: Phan Tuấn Minh**

**Lab Due Date: 14/9/2021**

**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), Find a CVE related to and scores that base on NIST Vul Database

Example: <https://nvd.nist.gov/vuln/detail/CVE-2020-14009> - CVE-2020-14009:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | CVE | Link | From lab #1 list | Severity |
| 1 | CVE-2020-14009 | <https://nvd.nist.gov/vuln/detail/CVE-2020-14009> | User downloads and unknown email attachment | HIGH |
| 2 | CVE-2021-36093 | https://nvd.nist.gov/vuln/detail/CVE-2021-36093 | Denial attack of organized e-mail server | MEDIUM |
| 3 | CVE-2020-26251 | https://nvd.nist.gov/vuln/detail/CVE-2020-26251 | Loss of production data | MEDIUM |
| 4 | CVE-2021-3051 | https://nvd.nist.gov/vuln/detail/CVE-2021-3051 | Unauthorized access to organization owned Workstation | HIGH |
| 5 | CVE-2021-37193 | https://nvd.nist.gov/vuln/detail/CVE-2021-37193 | Workstation browser has software vulnerability | LOW |
| 6 | CVE-2017-18917 | https://nvd.nist.gov/vuln/detail/CVE-2017-18917 | Denial attack of organized e-mail server | HIGH |

1. Describe the 6 control objectives of COBIT P09 which are used as benchmarks for IT risk assessment and risk management?

PO9.1 IT Risk Management Framework

PO9.2 Establishment of Risk Context

PO9.3 Event Identification

PO9.4 Risk Assessment

PO9.5 Risk Response

PO9.6 Maintenance and Monitoring of a Risk Action Plan

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

Example:

**1. CVE-2020-14009**: User downloads and unknown email attachment

* **Confidentiality**: Low
* **Integrity**: Low
* **Availability**: Low

**2**. **CVE-2021-36093**: Denial attack of organized e-mail server

* **Confidentiality**: None
* **Integrity**: None
* **Availability**: Low

## 3. CVE-2020-26251: Loss of production data

* **Confidentiality**: None
* **Integrity**: Low
* **Availability**: None

**4. CVE-2021-3051:** Unauthorized access to organization owned Workstation

* **Confidentiality**: High
* **Integrity**: High
* **Availability**: High

**5. CVE-2021-37193 :** Workstation browser has software vulnerability

* **Confidentiality**: None
* **Integrity**: None
* **Availability**: None

**6. CVE-2017-18917 :** User downloads and unknown email attachment

* **Confidentiality**: Partial
* **Integrity**: None
* **Availability**: None