Lab #2: Align Risk, Threats, & Vulnerabilities to COBIT P09 Risk Management Controls

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 14/1/2023

Lab Assessment Questions

1. From the identified threats & vulnerabilities from Lab #1

- Denial of Service attack of organized e-mail server
  Nessus: High
- Loss of Production Data
  Nessus: Medium
- Unauthorized access to organization owned Workstation
  Nessus: High
- Workstation browser has software vulnerability
  Nessus: Low
- User downloads an unknown e-mail attachment
  Nessus: Low

2. For the above identified threats and vulnerabilities, which of the following COBIT P09 Risk Management control objectives are affected?

- P09.1 Risk Management Framework- A
- P09.2 Establishment of Risk Context – B
- P09.3 Event Identification – A and B
- P09.4 Risk Assessment –C, D, and E
- P09.5 Risk Response – None
- P09.6 Maintenance and Monitoring of a Risk Action Plan – None

3. From the identified threats & vulnerabilities from Lab #1, specify whether the threat or vulnerability impacts confidentiality – integrity – availability:

Name	Confidentiality	Integrity	Availability
Denial of Service attack of organized e-mail server		X	X
Loss of Production Data	X		X
Unauthorized access to organization owned Workstation		X	

Workstation browser has software vulnerability	X		X
User downloads an unknown e-mail attachment		X	

4. For each of the threats and vulnerabilities from Lab #1 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.
- Change passwords, close ports, and set mirror server and proxy server.
- Loss of Production Data
- Unauthorized access to organization owned
- Workstation browser has software vulnerability
- User downloads an unknown e-mail attachment

5. For each of the threats and vulnerabilities from Lab #1 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: Denial of Service attack of organized e-mail server

- Information: Threat
- Applications: Threat
- Infrastructure: Threat
- People: None

b. Threat or Vulnerability #2: Unauthorized access to organization owned Workstation

- Information: Threat
- Application: Vulnerability
- Infrastructure: Vulnerability
- People: Threat

c. Threat or Vulnerability #3: Workstation browser has software vulnerability

- Information: Vulnerability
- Application: Vulnerability
- Infrastructure: Vulnerability
- People: None

d. Threat or Vulnerability #4: User downloads an unknown e-mail attachment

- Information: Vulnerability
- Application: Vulnerability

- Infrastructure: Vulnerability
- People: Threat

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

7. Why is it important to address each identified threat or vulnerability from a C-I-A perspective?
- Because the CIA is a balancing act. When it's too secure, people don't use it, when it's not secure enough, people risk 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 need alignment because it helps you rank information's importance and usage. It will determine the level of the risk factor if it has been 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?
- That's what every famous company does. 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?
- Send emails, memos, set up a training class. The risk that can reach the user the fastest or the highest threat should be prioritized first

11. What is the purpose of using the COBIT risk management framework and approach?
- A comprehensive framework that helps companies achieve governance and management goals for enterprise information and technology (IT) assets. Simply put, it helps companies create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk and resource utilization.

12. 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.

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

14. 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 your view of all the possible risks.

15. What is the name of the organization who defined the COBIT P.09 Risk Management Framework Definition?
- The IT Governance Institute