Lab #2: Assessment Worksheet

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

Course Name: IAA202

Student Name: Trần Minh Triết

Instructor Name: Phạm Yên Thao

Lab Due Date: 19.05.2023

Overview

Think of the COBIT framework as a giant checklist for what an IT or Risk Management auditor 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)

Answer:

a. Denial of Service attack of organized e-mail server

   Nessus: High

b. Loss of Production Data

   Nessus: Medium

c. Unauthorized access to organization owned Workstation

   Nessus: High

d. Workstation browser has software vulnerability

   Nessus: Low

e. 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?

Answer:

PO9.1 IT Risk Management Framework – **A**

PO9.2 Establishment of Risk Context – **B**

PO9.3 Event Identification – **A and B**

PO9.4 Risk Assessment – **C, D, and E**

PO9.5 Risk Response – **None**

PO9.6 Maintenance and Monitoring of a Risk Action Plan – **None**

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:

Answer:

a. Denial of Service attack of organized e-mail server – **Integrity, Availability**

b. Loss of Production Data – **Confidentiality, Availability**

c. Unauthorized access to organization owned Workstation – **Integrity**

d. Workstation browser has software vulnerability – **Confidentiality, Availability**

e. User downloads an unknown e-mail attachment – **Integrity**

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?

Answer:

Denial of Service attack of organized e-mail server

Change passwords, close ports, and set mirror server and proxy server.

Loss of Production Data

Backup date, restore from previous point if necessary.

Unauthorized access to organization owned Workstation.

Set password to change after 90 days, set screen lockout for 10 minutes.

Workstation browser has software vulnerability.

Update browser, check, and auto ipdate everyday

User downloads an unknown e-mail attachment.

Set strength filtering, send memos.

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:

Answer:

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: Loss of Production Data
   - **Information –** Threat
   - **Applications –** Threat
   - **Infrastructure –** Threat
   - **People –** Treat to someone's job.

c. Threat or Vulnerability #3: Unauthorized access to organiztion owned Workstation.
   - **Information** – Threat
   - **Applications –** Vulnerability
   - **Infrastructure –** Vulnerability
   - **People** – Threat

d. Threat or Vulnerability #4:
   - **Information** – Vulnerability
   - **Applications –** Vulnerability
   - **Infrastructure** – Vulnerability
   - **People –** None

e. Threat or Vulnerability #5:
   - **Information** – Vulnerability
   - **Applications –** Vulnerability
   - **Infrastructure** – Vulnerability
   - **People –** Threat

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

Answer:

TRUE

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

Answer:

Addressing each identified threat or vulnerability from a C-I-A (Confidentiality, Integrity, Availability) perspective because it provides a comprehensive framework for evaluating and managing risks to an organization's information assets.

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?

Answer:

Organizations can prioritize their risk mitigation efforts, customize security measures to the unique requirements of each classification level, satisfy regulatory compliance requirements, and optimize resource allocation by coordinating the assessment of risk impact with a data classification standard. It offers a standardized and organized method for determining how risks will affect information assets, thereby improving the effectiveness of a company's risk management strategy overall.

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?

Answer:

To provide thorough coverage, aid in the identification of specific vulnerabilities, reduce risks to infrastructure and applications, prioritize remediation efforts, and support a defense-in-depth security approach, it is important to align the assessment of risk impact with server and application software vulnerability assessments and remediation plans. It guarantees a more reliable and efficient method of handling hazards related to the organization's technological environment.

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?

Answer:

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

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

Answer:

Comprehensive framework that assists enterprises in achieving their objectives for 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.

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

Answer:

Effectiveness is following the instructions of a specific job while efficiency is doing the instructions in less 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 related to information systems security.

Answer:

Assesing the risk, Mitigatin 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?

Answer:

Organizations can adopt a comprehensive perspective of risks and their potential repercussions thanks to the COBIT P.09 framework. It makes sure that risk management initiatives support organizational objectives, are financially viable, uphold good customer relations, optimize internal procedures, and promote learning and development. This all-encompassing strategy improves the organization's capacity to recognize, rank, and effectively manage risks, ultimately boosting its resilience and long-term success.

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

Answer:

The IT Governance Institute