Lab #2: Assessment Worksheet

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

Course Name: IAA202

Student Name: Dang Hoang Nguyen

Instructor Name: Mrs. Pham Yen Thao

Lab Due Date: May 19, 2023

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. User downloads an unknown e –mail attachment: high

   b. User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers: medium

   c. Workstation browser has software vulnerability: low

   d. Service provider has a major network outage: low

   e. User destroys data in application and deletes all files: medium

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 – d
   - PO9.3 Event Identification – a, c

- PO9.4 Risk Assessment – a, b, e
- PO9.5 Risk Response – none of them
- PO9.6 Maintenance and Monitoring of a Risk Action Plan – none of them

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:

	Confidentiality	Integrity	Availability
A	x	x	
B	x		x
C	x	x	
D			x
E		x	x

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?

a. User downloads an unknown e-mail attachment:

- Assess the likelihood of users downloading unknown email attachments by reviewing security logs and user behavior patterns.
- Evaluate the potential impact of malware infection on systems and data by conducting a risk assessment.
- Review existing controls, including antivirus software and user awareness training, to determine their effectiveness.
- Consider implementing additional controls, such as email filtering and sandboxing technology, to further reduce the risk.
- Conduct a cost-benefit analysis to determine the most effective approach to mitigating this risk.

b. User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers:

- Assess the likelihood of users inserting personal devices into organization-owned computers by reviewing security logs and user behavior patterns.
- Evaluate the potential impact of malware infection on systems and data by conducting a risk assessment.
- Review existing controls, including access controls and user awareness training, to determine their effectiveness.

- Consider implementing additional controls, such as device scanning and encryption technology, to further reduce the risk.
- Conduct a cost-benefit analysis to determine the most effective approach to mitigating this risk.

c. Workstation browser has software vulnerability:

- Assess the likelihood of workstations having software vulnerabilities by reviewing security logs and vulnerability scan reports.
- Evaluate the potential impact of exploit on systems and data by conducting a risk assessment.
- Review existing controls, including patch management and access controls, to determine their effectiveness.
- Consider implementing additional controls, such as intrusion detection technology and web application firewalls, to further reduce the risk.
- Conduct a cost-benefit analysis to determine the most effective approach to mitigating this risk.

d. Service provider has a major network outage:

- Assess the likelihood of service providers experiencing major network outages by reviewing service level agreements and provider performance history.
- Evaluate the potential impact of downtime on critical services and operations by conducting a risk assessment.
- Review existing controls, including backup and recovery procedures and alternative service providers, to determine their effectiveness.
- Consider implementing additional controls, such as redundant network connections and failover systems, to further reduce the risk.
- Conduct a cost-benefit analysis to determine the most effective approach to mitigating this risk.

e. User destroys data in application and deletes all files:

- Assess the likelihood of users unintentionally or maliciously deleting data by reviewing security logs and user behavior patterns.
- Evaluate the potential impact of data loss on operations and compliance by conducting a risk assessment.
- Review existing controls, including access controls and data backups, to determine their effectiveness.
- Consider implementing additional controls, such as version control and audit trails, to further reduce the risk.
- Conduct a cost-benefit analysis to determine the most effective approach to mitigating this risk.

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: The risk impact on information is high since the attachment may contain malware or virus that can infect the system, leading to data loss or breach.

      • Applications: The risk impact on applications is high as well because the malware can spread and infect other applications, causing them to malfunction or become unusable.

      • Infrastructure: The risk impact on infrastructure is also high because the malware can spread to servers and other critical systems, leading to downtime or disruption of services.

      • People: The risk impact on people is moderate since users may lose access to their data or experience disruptions in their work.

   b. Threat or Vulnerability #2:

      • Information: The risk impact on information is low, as personal photos, music, and videos do not contain sensitive information.

      • Applications: The risk impact on applications is low as well, since the files are unlikely to contain malware that can affect the applications.

      • Infrastructure: The risk impact on infrastructure is low since the files are unlikely to infect servers or other critical systems.

      • People: The risk impact on people is moderate since users may waste time accessing personal files during work hours.

   c. Threat or Vulnerability #3:

      • Information: The risk impact on information is low since the vulnerability may not necessarily lead to data loss or breach.

      • Applications: The risk impact on applications is low, as the vulnerability may not affect the proper functioning of applications.

      • Infrastructure: The risk impact on infrastructure is low since the vulnerability may not affect servers or other critical systems.

      • People: The risk impact on people is low, as users may not experience any disruptions in their work.

   d. Threat or Vulnerability #4:

      • Information: The risk impact on information is low since the outage may not necessarily lead to data loss or breach.

• Applications: The risk impact on applications is moderate since the applications may become unavailable during the outage.

• Infrastructure: The risk impact on infrastructure is high since the outage may affect critical systems and cause downtime or disruption of services.

• People: The risk impact on people is high since users may lose access to their data and experience delays or disruptions in their work.

e. Threat or Vulnerability #5:

• Information: The risk impact on information is high since the data loss may result in a breach of sensitive information or loss of critical data.
• Applications: The risk impact on applications is high since the loss of data can affect the proper functioning of the applications.
• Infrastructure: The risk impact on infrastructure is moderate since the loss of data can affect critical systems and cause downtime or disruption of services.
• People: The risk impact on people is high since users may lose access to their data and experience delays or disruptions in their work.

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?

   CIA is short for Confidential, Integrity, Availability, it will help organizations prioritize their security efforts and allocate resources effectively. It also mitigates the most critical risks first

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?

   By doing the data classification standard, you will know which data is important, which will not. You will know the varying levels of sensitivity and require different levels of protection. It can can help you assess the risk impact on your information assets by providing a framework for categorizing data based on its level of importance and sensitivity, and determining the appropriate security controls for each category. This helps to ensure that resources are allocated appropriately to protect the most critical information assets from potential threats or vulnerabilities

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?

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?

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

    Using COBIT risk management framework and approach can help the IT company can do some complex tasks by identifying, assessing, evaluating, and responding to these risks in a structured and systematic manner.

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

    In this context, the effectiveness is talking about what we can achieve when we have the outcome. Meanwhiles efficiency is talking about the least number of resources we have to pay when having the result. Hence, in this case, effectiveness in assessing and risk management is talking about how well we do in identifying, assessing, evaluating, and responding to these risks, and efficiency is talking about the money, the time we have paid for the result.

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?

    APO13 - Manage security

    APO12 - Manage risk

    DSS05 - Manage security services

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

    Because it helps the organizations understand the potential impact of risks on their business objectives, IT objectives, compliance objectives, and overall risk posture. This holistic view helps organizations develop a more effective and efficient risk management strategy that addresses all aspects of their operations.

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

    ISACA (Information Systems Audit and Control Association)