Lab #2: Assessment Worksheet

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

Course Name: IAA202

Student Name: Phạm Thành Long

Instructor Name: Mai Hoàng Đỉnh

Lab Due Date: 19/09/2024

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. Unauthorized access from public Internet – **HIGH**
   Risk: Exposure of internal systems to external attacks, sensitive data theft, system compromise.
   b. Intra-office employee romance gone bad – **LOW**
   Risk: Typically an HR issue, unlikely to affect IT security directly but could lead to insider threats.
   c. Workstation OS has a known software vulnerability – **HIGH**
   Risk: Endpoint compromise, potential for malware or remote code execution.
   d. Workstation browser has software vulnerability – **MEDIUM**
   Risk: Potential for browser-based attacks (e.g., phishing, malware), data compromise.
   e. User downloads an unknown email attachment – **MEDIUM**
   Risk: Malware/ransomware infection, phishing attack, or system compromise.

2. For the above identified threats and vulnerabilities, which of the following COBIT P09 Risk Management control objectives are affected?
   a. Unauthorized access from public Internet – **HIGH**
   - **PO9.3 Event Identification** – Detect unauthorized access attempts.
   - **PO9.4 Risk Assessment** – Assess the risk of external attacks.
   - **PO9.5 Risk Response** – Implement strong firewalls, IDS/IPS systems.

- **PO9.6 Maintenance and Monitoring of a Risk Action Plan** – Continuously monitor for external threats.

b. Intra-office employee romance gone bad – **LOW**

- **PO9.2 Establishment of Risk Context** – Define potential HR-related risks affecting IT security.
- **PO9.4 Risk Assessment** – Assess the potential for insider threats.
- **PO9.5 Risk Response** – Implement access control measures to prevent misuse.

c. Workstation OS has a known software vulnerability – **HIGH**

- **PO9.3 Event Identification** – Identify vulnerable workstations.
- **PO9.4 Risk Assessment** – Evaluate the risk posed by unpatched vulnerabilities.
- **PO9.5 Risk Response** – Patch the OS or implement mitigations.
- **PO9.6 Maintenance and Monitoring of a Risk Action Plan** – Regularly update workstations and monitor for new vulnerabilities.

d. Workstation browser has software vulnerability – **MEDIUM**

- **PO9.3 Event Identification** – Detect browsers with outdated or vulnerable versions.
- **PO9.4 Risk Assessment** – Assess the likelihood of browser-based attacks.
- **PO9.5 Risk Response** – Apply security updates and browser hardening policies.
- **PO9.6 Maintenance and Monitoring of a Risk Action Plan** – Ensure that browser updates are regularly applied.

e. User downloads an unknown email attachment – **MEDIUM**

- **PO9.3 Event Identification** – Detect suspicious or malicious email attachments.
- **PO9.4 Risk Assessment** – Evaluate the impact of phishing or malware through email.
- **PO9.5 Risk Response** – Implement email security tools like anti-phishing filters.
- **PO9.6 Maintenance and Monitoring of a Risk Action Plan** – Continuously scan email attachments for malware.

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.

a. Unauthorized access from public Internet – **HIGH**

- **Confidentiality** – Unauthorized users may access sensitive data, violating confidentiality.
- **Integrity** – An attacker could alter or corrupt sensitive data.
- **Availability** – Systems might become unavailable if an attacker disrupts services.

b. Intra-office employee romance gone bad – **LOW**

- **Confidentiality** – Potential for insider threats, leaking confidential data.
- **Integrity** – Insider actions could alter or delete data maliciously.
- **Availability** – Less likely to directly impact availability unless used to sabotage systems.

c. Workstation OS has a known software vulnerability – **HIGH**

- **Confidentiality** – Exploiting the vulnerability could allow unauthorized data access.
- **Integrity** – The attacker could alter or manipulate workstation data.
- **Availability** – If compromised, the workstation could be disabled, affecting availability.

d. Workstation browser has software vulnerability – **MEDIUM**

- **Confidentiality** – Attacks such as phishing could compromise user credentials or sensitive data.
- **Integrity** – Malicious code could be introduced, altering data or web applications.
- **Availability** – The browser or system may become unstable or unusable due to an exploit.

e. User downloads an unknown email attachment – **MEDIUM**

- **Confidentiality** – Malware could extract sensitive information or send it to an attacker.
- **Integrity** – Ransomware or malicious software could corrupt or alter important files.
- **Availability** – Ransomware may lock users out of their files, impacting availability.

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. Unauthorized access from public Internet – **HIGH**

- **Risk Identification (PO9.3)** – Ensure the organization continues to identify any new external threats that could lead to unauthorized access. Regularly review access control logs and identify any suspicious activity.
- **Risk Assessment (PO9.4)** – Assess the effectiveness of firewalls, intrusion detection/prevention systems (IDS/IPS), and any additional security measures like VPN or multifactor authentication. Evaluate the likelihood and impact of external attacks on critical systems.
- **Risk Response (PO9.5)** – Confirm that mitigation measures, such as stronger access control policies, firewalls, and encryption for sensitive data, are in place and functioning effectively. Assess the speed and effectiveness of response strategies for unauthorized access incidents.
- **Maintenance and Monitoring (PO9.6)** – Monitor the external threat landscape and ensure that security measures are regularly updated (e.g., firewall configurations, access control lists). Perform ongoing reviews and penetration tests to ensure the infrastructure is secure.

b. Intra-office employee romance gone bad – **LOW**

- **Risk Identification (PO9.3)** – Identify risks related to insider threats arising from personnel issues. While low, these risks may still impact data security if access privileges are misused.
- **Risk Assessment (PO9.4)** – Assess the potential for insider misuse of access or data due to personal conflicts. Consider the impact on data confidentiality and integrity, particularly if sensitive data could be exposed.
- **Risk Response (PO9.5)** – Review access control measures to ensure that access to sensitive data is strictly controlled and monitored. Implement employee behavior monitoring tools if necessary to detect abnormal activities.
- **Maintenance and Monitoring (PO9.6)** – Continuously monitor employee access to sensitive systems and data. Regularly review and update HR and IT policies to address potential insider threats and ensure that any personal issues do not escalate into security incidents.

c. Workstation OS has a known software vulnerability – **HIGH**

- **Risk Identification (PO9.3)** – Continuously identify vulnerabilities in workstation operating systems through vulnerability scanning and vendor advisories. Regularly review the patching status of all systems.

- **Risk Assessment (PO9.4)** – Evaluate the risk of leaving known vulnerabilities unpatched, especially on critical systems. Consider the potential impact on data confidentiality, integrity, and availability.
- **Risk Response (PO9.5)** – Assess the implementation of patch management policies. Ensure that patches are applied in a timely manner and that any potential risks from unpatched systems are mitigated with compensating controls, like endpoint security software.
- **Maintenance and Monitoring (PO9.6)** – Monitor the patch management process to ensure updates are consistently applied. Continuously assess the need for additional mitigations, such as virtual patching or configuration management, to reduce risks from zero-day vulnerabilities.

d. Workstation browser has software vulnerability – **MEDIUM**

- **Risk Identification (PO9.3)** – Ensure vulnerabilities in workstation browsers are regularly identified through software updates and browser security advisories. Monitor browser usage for outdated or unsupported versions.
- **Risk Assessment (PO9.4)** – Assess the risk of browser-based attacks, such as phishing or drive-by downloads, particularly on workstations used for sensitive activities like finance or HR. Consider both the likelihood and potential damage of browser vulnerabilities.
- **Risk Response (PO9.5)** – Assess the browser update strategy and policies for preventing insecure browser configurations or plugins. Implement security extensions (e.g., ad blockers or script blockers) and enforce security policies like blocking vulnerable plugins or disabling untrusted sites.
- **Maintenance and Monitoring (PO9.6)** – Continuously monitor browser usage, ensure updates are applied regularly, and enforce browser security policies. Periodically reassess the risk of browser vulnerabilities as part of the overall security posture.

e. User downloads an unknown email attachment – **MEDIUM**

- **Risk Identification (PO9.3)** – Identify risks associated with email attachments, particularly phishing emails and malware. Use automated email filtering and anti-malware scanning systems to detect and block suspicious attachments.
- **Risk Assessment (PO9.4)** – Assess the risk of malware infection or ransomware attacks from untrusted email attachments. Evaluate the likelihood of such events and the potential impact on critical systems and data.
- **Risk Response (PO9.5)** – Review the effectiveness of email filtering systems and employee training programs on recognizing suspicious attachments. Ensure anti-malware systems are up to date and regularly tested. Implement backup and recovery strategies to mitigate the effects of ransomware.
- **Maintenance and Monitoring (PO9.6)** – Continuously monitor email traffic for new phishing or malware campaigns. Regularly test the organization's incident response to malware and review employee awareness through ongoing training and simulated phishing exercises.

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: Unauthorized access from public Internet – **HIGH**

      - **Information** –
        Risk Impact: Exposure of sensitive internal data.

Mitigation: Implement encryption (e.g., SSL/TLS) and access controls.

- **Applications** –
  Risk Impact: Disruption of critical business applications.
  Mitigation: Use firewalls and multi-factor authentication.
- **Infrastructure** –
  Risk Impact: Compromise of network infrastructure leading to system failures.
  Mitigation: Harden network devices, patch vulnerabilities, and use IDS/IPS.
- **People** –
  Risk impact: Employees may expose systems through misconfigurations.
  Mitigation: Train employees on secure remote access practices.

b. Threat or Vulnerability #2: Intra-office employee romance gone bad – **LOW**

- **Information** –
  Risk Impact: Potential insider threat leading to data misuse.
  Mitigation: Implement role-based access control and monitoring.
- **Applications** –
  Risk Impact: Misuse of applications or data due to personal grievances.
  Mitigation: Enforce RBAC and audit logs for sensitive systems.
- **Infrastructure** –
  Risk Impact: Disgruntled employees may attempt to sabotage systems.
  Mitigation: Limit administrative access and use multi-level authorization.
- **People** –
  Risk Impact: Personal issues between employees could lead to insider threats.
  Mitigation: Educate employees on security policies and enforce consequences for misuse.

c. Threat or Vulnerability #3: Workstation OS has a known software vulnerability – **HIGH**

- **Information** –
  Risk Impact: Data leakage or unauthorized access to sensitive data.
  Mitigation: Regularly patch the OS and use endpoint protection.
- **Applications** –
  Risk Impact: Potential disruption of business applications via malware.
  Mitigation: Implement application whitelisting and regular updates.
- **Infrastructure** –
  Risk Impact: Attackers may pivot from the compromised workstation to other systems.
  Mitigation: Segment the network and use endpoint isolation.
- **People** –
  Risk Impact: Unaware users may worsen the risk by not updating their systems.
  Mitigation: Train users on the importance of updates and patching.

d. Threat or Vulnerability #4: Workstation browser has software vulnerability – **MEDIUM**

- **Information** –
  Risk Impact: Theft of sensitive user credentials and session data.
  Mitigation: Ensure regular browser updates and use secure browsing practices.
- **Applications** –
  Risk Impact: Compromised browsers may lead to attacks on web-based applications.
  Mitigation: Enforce browser security policies and enable MFA for apps.
- **Infrastructure** –

Risk Impact: Browser vulnerabilities may open pathways for malware attacks.
Mitigation: Use sandboxing for browsers and monitor traffic for anomalies.

- **People** –
  Risk Impact: Users may visit malicious websites, increasing the risk of compromise.
  Mitigation: Train users on secure browsing habits and use web filters.

e. Threat or Vulnerability #5: User downloads an unknown email attachment – MEDIUM

- **Information** –
  Risk Impact: Potential loss or corruption of sensitive data.
  Mitigation: Use email security filters and malware scanning for attachments.
- **Applications** –
  Risk Impact: Malware may disrupt critical business applications.
  Mitigation: Implement strict email policies and anti-malware software.
- **Infrastructure** –
  Risk Impact: Infected workstations could spread malware across the network.
  Mitigation: Use network segmentation and endpoint monitoring.
- **People** –
  Risk impact: Employees may unknowingly download malicious content.
  Mitigation: Provide regular phishing and email security training.

6. True or False – COBIT P09 Risk Management controls objectives focus on assessment and management of IT risk.
   True
   COBIT P09 Risk Management control objectives focus on the assessment and management of IT risk. These objectives guide organizations in identifying, assessing, responding to, and monitoring IT risks to ensure they are managed effectively.

7. Why is it important to address each identified threat or vulnerability from a C-I-A perspective?
   Confidentiality, Integrity, and Availability (C-I-A) are fundamental principles of information security:

   a. Confidentiality:
   - Importance: Protects sensitive data from unauthorized access.
   - Benefit: Prevents data breaches and maintains privacy.

   b. Integrity:
   - Importance: Ensures data accuracy and prevents unauthorized modifications.
   - Benefit: Maintains trust and reliability in data and systems.

   c. Availability:
   - Importance: Ensures systems and data are accessible to authorized users when needed.
   - Benefit: Avoids disruptions and ensures business continuity.

   Addressing threats and vulnerabilities from a C-I-A perspective ensures comprehensive protection of data and systems, addressing risks to data confidentiality, integrity, and availability effectively.

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?

Importance of Alignment:

a. **Prioritization of Risks:** Focuses resources on protecting the most sensitive and critical information based on its classification.
b. **Relevant Impact Analysis:** Ensures risk impacts are assessed according to data sensitivity, leading to accurate risk management.
c. **Compliance:** Helps meet legal and regulatory requirements for data protection.
d. **Consistent Protection:** Tailors security measures to the specific needs of different data classifications.
e. **Accountability:** Clarifies responsibility for managing and mitigating risks associated with various data types.

How data classification standard helps:

a. **Defines Sensitivity Levels:** Guides the assessment of potential impacts on sensitive data.
b. **Directs Security Measures:** Informs appropriate controls based on data classification.
c. **Helps in Risk Prioritization:** Focuses risk management efforts on the most critical information.
d. **Aligns with Compliance Needs:** Ensures adherence to data protection regulations and standards.

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?

Importance of Alignment:

a. **Comprehensive Risk Management:**
   - Reason: Applications and infrastructure can have different vulnerabilities that affect their security and performance.
   - Benefit: Aligning risk assessments with both server and application vulnerability assessments ensures that all potential threats are identified and addressed.

b. **Targeted Remediation:**
   - Reason: Different types of vulnerabilities require specific remediation approaches.
   - Benefit: A combined approach ensures that both server and application vulnerabilities are patched effectively, reducing overall risk.

c. **Improved Security Posture:**
   - Reason: Comprehensive assessments and remediation plans cover various aspects of the IT environment.
   - Benefit: This approach enhances the overall security posture by addressing vulnerabilities in both the server infrastructure and application layers.

d. **Efficient Resource Allocation:**
   - Reason: Knowing the specific vulnerabilities helps prioritize remediation efforts.
   - Benefit: Aligning assessments allows for more efficient use of resources, focusing on the most critical vulnerabilities first.

e. **Compliance and Best Practices:**

- Reason: Regulations and security best practices often require thorough vulnerability assessments and remediation.
- Benefit: Ensures compliance and aligns with industry standards, mitigating legal and operational risks.