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

Lab #2: Assessment Worksheet

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

Course Name: IAA202

Student Name: Huynh Ngoc Quang

Instructor Name: Mr. Mai Hoang Dinh

Lab Due Date: September 18, 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. 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. User destroys data in application and deletes all files: **High**
    d. LAN server OS has a known software vulnerability: **High**
    e. Service provider has a major network outage: **Low**
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 – **none**
    - PO9.2 Establishment of Risk Context – d
    - PO9.3 Event Identification – a, b, c

- PO9.4 Risk Assessment – a, b, c, d, e
- PO9.5 Risk Response – a, b, c, d, e
- PO9.6 Maintenance and Monitoring of a Risk Action Plan – a, b, c, d

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	✓		
b	✓		
c		✓	✓
d	✓		
e			✓

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 email attachment:
        - Risk Awareness and Training: Assess the effectiveness of training programs regarding email security.
        - Monitoring and Detection: Evaluate systems in place for detecting and mitigating phishing attempts.
        - Incident Response: Review the incident response plan for handling suspicious downloads.
    b. User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers:
        - Access Control Policies: Assess the enforcement of policies regarding the use of external devices.
        - Data Loss Prevention (DLP): Evaluate the effectiveness of DLP solutions to monitor and control data transfer.
        - User Behavior Monitoring: Implement monitoring solutions to detect unauthorized device usage.
    c. User destroys data in application and deletes all files:
        - Data Backup and Recovery: Assess the robustness of backup systems to recover lost data.
        - Audit Logs and Monitoring: Evaluate the effectiveness of logging and monitoring changes to critical data.
        - User Access Controls: Review access permissions to sensitive applications and data.

d. LAN server OS has a known software vulnerability:
   - Patch Management Process: Assess the timeliness and effectiveness of the patch management process.
   - Vulnerability Scanning: Regularly assess systems for known vulnerabilities and track remediation efforts.
   - Configuration Management: Review configurations to ensure compliance with security best practices.

e. Service provider has a major network outage:
   - Business Continuity Planning: Assess the effectiveness of the business continuity plan in the event of service outages.
   - SLAs with Service Providers: Review service level agreements for clarity on uptime and support during outages.
   - Redundancy and Failover Mechanisms: Evaluate the implementation of redundancy in network architecture.

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: User downloads an unknown email attachment
      - Information:
        - Risk Impact: Sensitive data may be compromised, leading to potential data breaches.
        - Mitigation: Implement data loss prevention (DLP) solutions and enforce encryption for sensitive data.
      - Applications
        - Risk Impact: Malware may corrupt or exploit applications, leading to unauthorized access.
        - Mitigation: Utilize application whitelisting and ensure all software is regularly updated and patched.
      - Infrastructure
        - Risk Impact: The network may be compromised, affecting the integrity of other systems.
        - Mitigation: Employ network segmentation and use intrusion detection/prevention systems (IDS/IPS) to monitor for malicious activity.
      - People
        - Risk Impact: Users may inadvertently become attack vectors, impacting organizational security culture.

        - Mitigation: Provide ongoing training and phishing simulations to educate users about identifying suspicious emails.

b. Threat or Vulnerability #2: User inserts CDs and USB hard drives with personal photos, music, and videos on organization-owned computers
    - Information
        - Risk Impact: Risk of data leakage and potential malware introduction through unverified devices.
        - Mitigation: Implement strict access controls on USB ports and enforce policies prohibiting personal devices.
    - Applications
        - Risk Impact: Unauthorized applications or malware may be introduced to the organization's systems.
        - Mitigation: Use application control mechanisms to restrict the execution of unapproved software.
    - Infrastructure
        - Risk Impact: Potential for malware to spread across the network, affecting overall infrastructure integrity.
        - Mitigation: Regularly update antivirus solutions and scan all devices before connecting them to the network.
    - People
        - Risk Impact: Users may unintentionally expose the organization to risks by using personal devices.
        - Mitigation: Conduct training on safe device usage and establish clear policies regarding personal devices in the workplace.
c. Threat or Vulnerability #3: User destroys data in application and deletes all files
    - Information
        - Risk Impact: Permanent loss of critical data, affecting operations and compliance.
        - Mitigation: Implement regular automated backups and a robust data recovery plan.
    - Applications
        - Risk Impact: Application functionality may be severely impacted due to missing data.
        - Mitigation: Ensure version control and data integrity checks are in place for critical applications.
    - Infrastructure

        - Risk Impact: Possible disruption of services due to data loss, affecting system availability.
        - Mitigation: Utilize redundancy strategies for critical infrastructure components to ensure service continuity.
    - People
        - Risk Impact: Users may feel frustrated or demotivated due to data loss, impacting productivity.
        - Mitigation: Foster a culture of accountability and provide training on proper data handling and recovery procedures.

d. Threat or Vulnerability #4: LAN server OS has a known software vulnerability
    - Information
        - Risk Impact: Increased risk of data breaches and unauthorized access to sensitive information.
        - Mitigation: Regularly conduct vulnerability assessments and patch management to address known vulnerabilities.
    - Applications
        - Risk Impact: Exploits may compromise application integrity and functionality.
        - Mitigation: Monitor application security and ensure all applications are kept up-to-date with security patches.
    - Infrastructure
        - Risk Impact: The entire network could be compromised if a vulnerability is exploited.
        - Mitigation: Implement network monitoring tools to detect unusual activities and segment networks to contain potential breaches.
    - People
        - Risk Impact: IT staff may be overwhelmed by incidents arising from vulnerabilities, affecting morale.
        - Mitigation: Provide adequate resources and training to ensure staff can effectively manage and remediate vulnerabilities.

e. Threat or Vulnerability #5: Service provider has a major network outage
    - Information
        - Risk Impact: Potential loss of access to critical data and services, impacting business operations.
        - Mitigation: Develop a business continuity plan that includes strategies for accessing critical information during outages.
    - Applications

    - Risk Impact: Applications reliant on the service provider may become unavailable, disrupting operations.
    - Mitigation: Establish service level agreements (SLAs) with clear expectations for uptime and support.
- Infrastructure
    - Risk Impact: Overall service delivery may be impacted, leading to operational delays and loss of productivity.
    - Mitigation: Implement redundancy and failover solutions to maintain services during outages.
- People
    - Risk Impact: Employees may experience frustration and decreased productivity due to service interruptions.
    - Mitigation: Communicate effectively with staff about expected downtimes and provide support during outages.

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

   True. COBIT PO9 Risk Management control objectives focus on the assessment and management of IT risk, ensuring that IT-related risks are identified, evaluated, and effectively managed to align with business objectives and enhance overall governance.
7. Why is it important to address each identified threat or vulnerability from a C-I-A perspective?

   Because it ensures a comprehensive security approach.
    - Confidentiality: Protects sensitive data from unauthorized access, reducing the risk of breaches.
    - Integrity: Ensures data accuracy and reliability, preventing unauthorized alterations that could lead to misinformation or fraud.
    - Availability: Guarantees that data and services are accessible when needed, minimizing downtime and operational disruption.

   By evaluating threats through this lens, organizations can prioritize and implement effective security measures that safeguard all aspects of their 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?
    - Prioritization: The Data Classification Standard categorizes data based on its sensitivity and importance. This helps prioritize which assets require more rigorous protection measures based on potential impact.

- Regulatory Compliance: Many regulations mandate specific protections based on data classification. Aligning assessments helps ensure compliance and reduces legal risks.
- Consistent Framework: It provides a consistent framework for evaluating risks, ensuring that all data is assessed uniformly, leading to more reliable and comparable results.

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?
    - Resource Allocation: This alignment helps in allocating resources effectively, ensuring that the most critical vulnerabilities are addressed first based on their potential impact.
    - Regulatory Compliance and Best Practices: It aligns with industry best practices and compliance requirements, ensuring that both applications and infrastructure meet necessary security standards.
    - Targeted Remediation: Understanding specific vulnerabilities allows for targeted remediation strategies, prioritizing fixes based on the risk they pose to applications and infrastructure.
    - Comprehensive Coverage: It ensures that all aspects of the environment are evaluated, addressing both the applications and underlying infrastructure, which could be interdependent.
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?
    - Regular Updates: Establish a communication channel (e.g., email alerts, intranet updates) to keep users informed about ongoing threats and mitigation efforts.
    - Training Sessions: Conduct training or awareness sessions to educate users on recognizing potential threats and understanding their role in maintaining security.
    - Incident Reports: Share detailed reports post-incident to explain what was done to mitigate the threat and how it affects their work.
    - User Impact: Assess how the vulnerability affects users and their daily operations. Prioritize those that disrupt productivity or expose sensitive data.

- Compliance Requirements: Identify vulnerabilities that may violate regulatory requirements, prioritizing remediation to ensure compliance.

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

To provide organizations with a structured method for managing IT-related risks. Key benefits include:

- Holistic Risk Management: COBIT offers a comprehensive framework that integrates risk management with governance and management of enterprise IT.
- Regulatory Compliance: COBIT supports compliance with legal, regulatory, and industry standards by providing a structured approach to risk management.
- Performance Measurement: The framework includes performance metrics to evaluate the effectiveness of risk management efforts and to drive continuous improvement.
- Improved Decision-Making: By assessing risks within a defined framework, organizations can make more informed decisions regarding risk acceptance, mitigation, and transfer.

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

Effectiveness measures how well risk management achieves its intended outcomes, focusing on reducing risks and preventing incidents.

Efficiency assesses how resources are utilized in the process, emphasizing cost-effectiveness and resource optimization.

In summary, effectiveness is about achieving the right results, while efficiency is about doing so with optimal resource use. Both are crucial for effective risk management.

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?
    a. Governance: Establishes frameworks and policies for managing IT risks, ensuring alignment with organizational objectives and compliance requirements.
    b. Risk Assessment: Involves identifying, analyzing, and evaluating risks to information systems, helping prioritize vulnerabilities based on their potential impact.

c. Incident Management: Focuses on detecting, responding to, and recovering from security incidents, ensuring that organizations can effectively mitigate damage and learn from events.

14. Why is it important to assess risk impact from four different perspectives as part of the COBIT P.09 Framework?
    a. Comprehensive Understanding: Evaluating risks from multiple perspectives (strategic, operational, financial, and compliance) provides a holistic view of potential impacts, ensuring that no critical aspect is overlooked.
    b. Informed Decision-Making: Different perspectives help stakeholders make better-informed decisions by understanding how risks affect various facets of the organization.
    c. Prioritization: It allows for effective prioritization of risks based on their significance to different areas, enabling targeted mitigation strategies that align with organizational goals.
    d. Stakeholder Alignment: Engaging various stakeholders in the risk assessment process fosters alignment and supports a unified approach to risk management across the organization.
15. What is the name of the organization who defined the COBIT P.09 Risk Management Framework Definition?

    COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for information technology (IT) management and IT governance.