Lab #2: Assessment Worksheet

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

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

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.
   b.
   c.
   d.
   e.

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 –
   - PO9.2 Establishment of Risk Context –

- PO9.3 Event Identification –
- PO9.4 Risk Assessment –
- PO9.5 Risk Response –
- PO9.6 Maintenance and Monitoring of a Risk Action Plan –

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?

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** –
      - **Applications** –
      - **Infrastructure** –
      - **People** –
   b. Threat or Vulnerability #2:
      - **Information** –
      - **Applications** –
      - **Infrastructure** –

- **People** –

c. Threat or Vulnerability #3:
   - **Information** –
   - **Applications** –
   - **Infrastructure** –
   - **People** –

d. Threat or Vulnerability #4:
   - **Information** –
   - **Applications** –
   - **Infrastructure** –
   - **People** –

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

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

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

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?

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?

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

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

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