# UNIVERSITI KUALA LUMPUR
## MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

## FINAL EXAMINATION
### JANUARY 2016 SEMESTER

| | | |
|---|---|---|
| COURSE CODE | : | IKB 42103 |
| COURSE NAME | : | IT SECURITY AUDIT AND ASSESSMENT |
| PROGRAMME NAME | : | BIT(HONS) IN COMPUTER SYSTEM SECURITY |
| DATE | : | 23 MAY 2016 |
| TIME | : | 2.00 pm – 4.30 pm |
| DURATION | : | 2 HOURS 30 MINUTES |



## INSTRUCTIONS TO CANDIDATES

1. Please CAREFULLY read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of TWO (2) sections; Section A and Section B.
4. Answer ALL questions in Section A. For Section B, answer ONE (1) question ONLY
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.

THERE ARE 6 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

**SECTION A (Total: 75 marks)**

**INSTRUCTION: Answer ALL questions.**
**Please use the answer booklet given.**

**Question 1**

(a) Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. In what ways must information be protected? Elaborate **THREE (3)** main characteristics of information.

(6 marks)

(b) In IT audit process, threat and vulnerabilities is the basic elements in accessing risk in the organization. Elaborate threat and vulnerabilities. How do you identify them?

(5 marks)

(c) In order to analyze risk, audits, security assessments, vulnerability scans, and penetration tests are the method use in security assessment. Briefly explain the scope for each of the way:

i. Audit
ii. Vulnerability scan
iii. Penetration test

(6 marks)

(d) Mutiara Sdn. Bhd. has three information assets to evaluate for risk management. Your team is required to calculate the risk for each asset using this formula: Risk = (Likelihood X value) – percentage + uncertainty. Show the calculation in detail.

Asset A: has impact value score of 50 and has one vulnerability. Vulnerability 1 has a likelihood of 1.0 with no current controls, & you estimate the assumptions and data are 90% accurate.

Asset B: has a value score of 100 and has 2 vulnerabilities. Vulnerability 2 has a likelihood of 0.5 with current controls address 50% of its risk, vulnerability 3 has a likelihood of 0.1 with no current controls, & you estimate the assumptions and data are 80% accurate

Asset C: This is a web server that deals with e-commerce transactions. It has one vulnerability with a likelihood of 0.1. However it has an impact rating of 100. Assumptions made on this asset have an 80% certainty.

(8 marks)

**Question 2**

(a) List **FOUR (4)** the most significant or common penetration tools that is being used to do penetration testing.

(2 marks)

(b) The type of penetration testing normally depends on the scope and the organizational wants and requirements. Commonly, there are three important types of pen testing. For each scenario given, briefly explain what kind of penetration testing or assessment is being performed.

i. You have just received an assignment for an assessment at a company site. Company's management is concerned about external threat and wants to take appropriate steps to insure security is in place. Anyway the management is also worried about possible threats coming from inside the site, specifically from employees belonging to different Departments.

(4 marks)

ii. A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test is done from an external IP address with no prior knowledge of the internal IT systems.

(4 marks)

(c) Open Source Security Testing Methodology Manual (OSSTMM) is a peer reviewed methodology for performing security tests and metrics.

i. OSSTMM defines the security map which is a visual representation of six different types of security tests distinguished in the methodology. List **SIX (6)** sections of security define in OSSTMM.

(6 marks)

ii. The OSSTMM test cases are divided into five sections. Indicate the **FIVE (5)** test sections.

(5 marks)

(b) In the security assessment, list **FOUR (4)** elements that must be included during assessment.

(4 marks)

**Question 3**

Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments.

(a) Discuss the **THREE (3)** importances of Common Criteria.

(6 marks)

(b) Briefly explain the **TWO (2)** key components of Common Criteria.

(4 marks)

(c) Briefly explain **THREE (3)** target audiences of Common Criteria.

(9 marks)

(d) Briefly explain what a Target of Evaluation (TOE) is.

(2 marks)

(e) List **FOUR (4)** examples of TOE's.

(4 marks)

**SECTION B (Total: 25 marks)**

**INSTRUCTION: Answer ONE (1) question ONLY.**
**Please use the answer booklet given.**

**Question 4**

(a) During the risk assessment process, your team is required to identify possible impact for asset based on the threat that has been identified earlier. Identify **TWO (2)** impacts that will be faced by the asset listed below:

| Asset | Threat | Impact |
|---|---|---|
| Payroll application | Masquerading of user identity by insiders | |
| Retirement application | Unauthorized use of an application | |
| Web portal | Embedding of malicious code | |
| Payroll data, retirement data, web portal data | User errors | |
| Payroll application, retirement application | Communications manipulation | |

(10 Marks)

(b) A lot of people use the words security audit, vulnerability assessment and penetration test interchangeably.

i. What will be the goal for each practice?

(3 marks)

ii. Briefly explain the differences between security audits, vulnerability assessment and penetration tests.

(6 marks)

iii. How these tests help promote a more secure environment?

(6 marks)

**Question 5**

(a) How often you should perform penetration testing? Support your answer by giving reason.

(3 marks)

(b) Identify the Threat-Source and the Threat Action for each vulnerability listed below:

i. Terminated employee's system ID are not removed from the system

(3 marks)

ii. Company firewall allows inbound telnet and guest ID enable on XYZ server

(3 marks)

iii. The vendor has identifies flaws in the security design of the system

(3 marks)

iv. Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place

(3 marks)

(c) Briefly explain **THREE (3)** importance of preparing vulnerability listing prior to the penetration testing.

(6 marks)

(d) List **FOUR (4)** sources where you can find technical vulnerabilities.

(4 marks)



**END OF EXAMINATION PAPER**