Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2022/2023

COURSE NAME	:	CRITICAL INFRASTRUCTURE SECURITY
COURSE CODE	:	BIS 33303
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	FEBRUARY 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER ALL QUESTIONS. 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK**. 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **SEVEN (7)** PAGES

SECTION A
Instruction: Choose the BEST answer for each of the following questions.

Q1 What is a methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes?

A. Penetration testing.
B. Auditing.
C. Risk analysis.
D. Entrapment.

(2 marks)

Q2 Failure to _____ can result in the perception that due care is not being maintained.

A. perform periodic security audits
B. deploy all available safeguards
C. assess performance reviews
D. create audit reports for shareholders

(2 marks)

Q3 What are used to inform would-be intruders or those who attempt to violate security policy that their intended activities are restricted and that any further activities will be audited and monitored?

A. Security policies.
B. Interoffice memos.
C. Warning banners.
D. Honey pots.

(2 marks)

Q4 Which of the following activities is **NOT** considered a valid form of penetration testing?

A. Denial of service attacks.
B. Port scanning.
C. Distribution of malicious code.
D. Packet sniffing.

(2 marks)

Q5 What is the term used to describe the responsibility of a firm's officers and directors to ensure that adequate measures are in place to minimize the effect of a disaster on the organization's continued viability?

A. Corporate responsibility.
B. Disaster requirement.
C. Due diligence.
D. Going concern responsibility.

(2 marks)

Q6 You are concerned about the risk that a flood poses to your RM3 million shipping facility. Based upon expert opinion, you determine that there is a 5 percent chance that a flood will occur each year. Experts advise you that an flood would completely destroy your building and require you to rebuild on the same land. Ninety percent of the RM3 million value of the facility is attributed to the building and 10 percent is attributed to the land itself.

What is the single loss expectancy of your shipping facility to flood?

A. RM3,000,000.
B. RM2,700,000.
C. RM270,000.
D. RM135,000.

(2 marks)

Q7 A server that houses sensitive data has been stored in an unlocked room for the last few years at Macaroni Datahouse Sdn Bhd. The door to the room has a sign on the door that reads "Room 1."

The fact that the server has been in an unlocked room marked "Room 1" for the last few years means the company was practicing which of the following?

A. Logical security.
B. Risk management.
C. Risk transference.
D. Security through obscurity.

(2 marks)

Q8 Which factor is the most important item when it comes to ensuring security is successful in an organization?

A. Senior management support
B. Effective controls and implementation methods
C. Updated and relevant security policies and procedures
D. Security awareness by all employees

(2 marks)

Q9 What type of plan outlines the procedures to follow when a disaster interrupts the normal operations of a business?

A. Business Continuity Plan.
B. Business Impact Assessment.
C. Disaster Recovery Plan.
D. Vulnerability Assessment.

(2 marks)

Q10 Which one of the following items is a characteristic of hot sites but **NOT** a characteristic of warm sites?

A. Communications circuits.
B. Workstations.
C. Servers.
D. Current data.

(2 marks)

Q11 Which one of the following statements about Business Continuity Planning and Disaster Recovery Planning is **NOT TRUE**?

A. Business Continuity Planning is focused on keeping business functions uninterrupted when a disaster strikes.
B. Organizations can choose whether to develop Business Continuity Planning or Disaster Recovery Planning plans.
C. Business Continuity Planning picks up where Disaster Recovery Planning leaves off.
D. Disaster Recovery Planning guides an organization through recovery of normal operations at the primary facility.

(2 marks)

Q12 What type of backup involves always storing copies of all files modified since the most recent full backup?

A. Differential backups.
B. Partial backup.
C. Incremental backups.
D. Database backup.

(2 marks)

Q13 What disaster recovery principle best protects your organization against hardware failure?

A. Consistency.
B. Efficiency.
C. Redundancy.
D. Primacy.

(2 marks)

Q14 When an employee is to be terminated, which of the following should be done?

A. Inform the employee a few hours before they are officially terminated.
B. Disable the employee's network access just before they are informed of the termination.
C. Send out a broadcast e-mail informing everyone that a specific employee is to be terminated.
D. Wait until you and the employee are the only people remaining in the building before announcing the termination.

(2 marks)

Q15 Which of the following would **NOT** be considered an asset in a risk analysis?

A. A development process.
B. An IT infrastructure.
C. A proprietary system resource.
D. Users' personal files.

(2 marks)

SECTION B

Q16 One of the most important security documents to support security program of a critical infrastructure is the Security Policy.

(a) Describe **FIVE (5)** most important characteristics of a Security Policy document.

(10 marks)

(b) Propose a hierarchy of security policies inside a Security Policy.

(5 marks)

Q17 There is a strong movement at the world level to remove high carbon generating energy due to Ozone layer depletion. Many countries have started to prepare alternative energy source.

Propose **TWO (2)** directions Malaysia should invest for alternative energy to support its growing industries and residents.

(4 marks)

Q18 Despite a well designed and implementation of all layers of defense, human remains the weakest point. Suggest **THREE (3)** possible countermeasures to reduce this vulnerability.

(6 marks)

Q19 The criticality of an infrastructure is measured based on the impact it has on a nation.

(a) On a scale of 6 criticality level, assign the criticality of **TEN (10)** critical infrastructure sectors in Malaysia.

(10 marks)

(b) Draw a dependency diagram between these infrastructures.

(4 marks)

(c) Based on **Q19(a)** and **Q19(b)**, identify the top **THREE (3)** critical infrastructure for Malaysia.

(2 marks)

Q20 Sabotage from terrorist, issue motivated groups and political motivated groups can seriously affect the operation of CIIP (Critical Information Infrastructure Protection).

Discuss **THREE (3)** other possible threats affecting the CIIP of a nation.

(9 marks)

- END OF QUESTIONS -