Universiti Tun Hussein Onn Malaysia

# UNIVERSITI TUN HUSSEIN ONN MALAYSIA

## FINAL EXAMINATION
## SEMESTER I
## SESSION 2019/2020

| | | |
|---|---|---|
| COURSE NAME | : | CRITICAL INFRASTRUCTURE SECURITY |
| COURSE CODE | : | BIS 33303 |
| PROGRAMME CODE | : | BIS |
| EXAMINATION DATE | : | DECEMBER 2019/JANUARY 2020 |
| DURATION | : | 3 HOURS |
| INSTRUCTION | : | ANSWER **ALL** QUESTIONS |



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

**SECTION A**

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

**Q1** _____ provides data for recreating step-by-step the history of an event, intrusion, or system failure.

A. Security policies
B. Log files
C. Audit reports
D. Business continuity planning

**Q2** Why should access to audit reports be controlled and restricted?

A. They contain copies of confidential data stored on the network.
B. They contain information about the vulnerabilities of the system.
C. They are useful only to upper management.
D. They include the details about the configuration of security controls.

**Q3** _____ 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

**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

**Q5** Searching through the refuse, remains, or leftovers from an organization or operation to discover or infer confidential information is known as _____.

A. Impersonation
B. Dumpster diving
C. Social engineering
D. Inference

**Q6** What is the first step that individuals responsible for the development of a Business Continuity Plan (BCP) should perform?

A. BCP team selection
B. Business organization analysis
C. Resource requirements analysis
D. Legal and regulatory assessment

**Q7** Which one of the following Business Impact Analysis (BIA) terms identifies the amount of money a business expects to lose to a given risk each year?

A. ARO
B. SLE
C. ALE
D. EF

**Q8** You are concerned about the risk that an avalanche poses to your $3 million shipping facility. Based upon expert opinion, you determine that there is a 5 percent chance that an avalanche will occur each year. Experts advise you that an avalanche would completely destroy your building and require you to rebuild on the same land. Ninety percent of the $3 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 avalanches?

A. $3,000,000
B. $2,700,000
C. $270,000
D. $135,000

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

A. Business Continuity Plan (BCP)
B. Business Impact Assessment
C. Disaster Recovery Plan (DRP)
D. Vulnerability assessment

**Q10** What is the end goal of Disaster Recovery Planning?

A. Preventing business interruption
B. Setting up temporary business operations
C. Restoring normal business activity
D. Minimizing the impact of a disaster

**Q11** What BCP technique can help you prepare the business unit prioritization task of Disaster Recovery Planning?

A. Vulnerability Analysis
B. Business Impact Assessment
C. Risk Management
D. Continuity Planning

**Q12** What is the typical time estimate to activate a warm site from the time a disaster is declared?

A. 1 hour
B. 6 hours
C. 12 hours
D. 24 hours

**Q13** 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

**Q14** What Disaster Recovery Planning tool can be used to protect an organization against the failure of a critical software firm to provide appropriate support for their products?

A. Differential backups
B. Business Impact Assessment
C. Incremental backups
D. Software escrow agreement

**Q15** 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

**Q16** Which of the following is the weakest element in any security solution?

A. Software products
B. Internet connections
C. Security policies
D. Humans

**Q17** 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.

**Q18** Which of the following is not an element of the risk analysis process?

A. Analyzing an environment for risks
B. Creating a cost/benefit report for safeguards to present to upper management
C. Selecting appropriate safeguards and implementing them
D. Evaluating each risk as to its likelihood of occurring and cost of the resulting damage

**Q19** 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

**Q20** When a safeguard or a countermeasure is not present or is not sufficient, what is created?

A. Vulnerability
B. Exposure
C. Risk
D. Penetration

(40 marks)

**SECTION B**

**Q21** Human is one of the most vulnerable point of attacks in a critical infrastructure. Suggest **THREE (3)** ways to change staff security behaviors so that an infrastructure is more prepared.

(20 marks)

**Q22** You are the person in charge of handling the CIIP (Critical Information Infrastructure Protection) in your organization.

(a) Differentiate between dependency and interdependency.

(6 marks)

(b) Discuss **ONE (1)** example of dependencies on any CIIP sectors.

(4 marks)

(c) Illustrate **THREE (3)** interdependencies using dependency diagram.

(10 marks)

**Q23** Compare and contrast the following concepts with appropriate example

(a) Strategic, tactical and operational plans.

(b) Security Standards, Guidelines and Security Procedures

(20 marks)

**- END OF QUESTIONS -**