Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2017/2018

COURSE NAME	:	INFORMATION SECURITY STANDARD
COURSE CODE	:	BIS 33203
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE / JULY 2018
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **EIGHT (8)** PAGES

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

Q1 Which of the following control known as unauthorized access?

A. Limiting the local access of operations personnel.
B. Enforcing auditing.
C. Enforcing separation of duties.
D. Limiting control of management personnel.

Q2 Generating magnetic fields to erase the content on a type of media is called _____.

A. Sniffing
B. Degaussing
C. Wiretapping
D. Magnetizing

Q3 When you approach a restricted facility, you are requested for identification and verified against a pre-approved list by the guard at the front gate before being let in.

This is an example of checking for the principle of _____.

A. Least privilege
B. Separation of duties
C. Fail-safe
D. Psychological acceptability

Q4 Within an organization the security officer detects that a workstation of an employee is infected with malicious software. The malicious software was installed due to a targeted Phishing attack.

Which action is the most beneficial to prevent such incidents in the future?

A. Implementation Mandatory Access Control (MAC) technology.
B. Update the firewall rules.
C. Start a security awareness program.
D. Update the signatures of the spam filter.

Q5 A worker from an insurance company discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this. She reports this security incident to the Helpdesk. The Helpdesk worker records the following information regarding this incident:

- Date and time,
- Description of the incident, and
- Possible consequences of the incident.

What is the most important information missing from the report?

A. The name of the person reporting the incident.
B. The name of the software package.
C. The Personal Computer (PC) number.
D. A list of people who were informed about the incident.

Q6 You work in the IT department of a medium-sized company. Confidential information has come into the wrong hands several times. This hurt the image of the company. You have been asked to propose organizational security measures for laptops at your company.

What is the first step that you should take?

A. Formulate a policy regarding mobile device.
B. Appoint security personnel.
C. Encrypt the hard disks of laptops and USB sticks.
D. Set up an access control policy.

Q7 An operations control that identifies potential fraudulent activity by requiring different personnel to switch job functions on a regular basis is called _____.

A. Mandatory vacation
B. Need-to-know
C. Separation of duties
D. Job rotation

Q8 Security is a (n) _____ process.

A. continuous
B. indicative
C. examined
D. abnormal

Q9 The major benefit of information classification is to _____.

A. map out the computing ecosystem
B. identify the threats and vulnerabilities
C. determine the software baseline
D. identify the appropriate level of protection needs

Q10 Which security model focuses on confidentiality only?

A. Biba.
B. Clark-Wilson.
C. Bell-LaPadula.
D. Information Flow.

Q11 When the Business Continuity Plan (BCP) should be reviewed?

A. Whenever encountering a disaster.
B. At least annually or whenever significant changes occur.
C. Whenever the company gets audited.
D. Whenever the legal department declares it is time.

Q12 _____ backup is performed when all files of the database are copied and the database is not available to users.

A. Old
B. Warm
C. Hot
D. Neutral

Q13 Computer security is generally considered to be the responsibility of _____.

A. everyone in the organization
B. corporate management
C. the corporate security staff
D. everyone with computer access

Q14 Strong authentication is needed to access highly protected areas. Which factor is verified when we must show our access card?

A. Something you are.
B. Something you have.
C. Something you know.
D. All of the mentioned.

Q15 What is the purpose of a business continuity plan (BCP)?

A. To keep business operations running.
B. To recover from a disaster.
C. To test the business continuity plan.
D. To develop the business continuity plan.

Q16 Operations departments should back up data in all of the following situations **EXCEPT** _____.

A. once per year
B. immediately following a reorganization
C. after a system upgrade
D. for authorized on-demand requests

Q17 Which of the followings is the **BEST** description of a digital signature?

A. The sender encrypts a message digest with his/her public key.
B. The sender encrypts a message digest with his/her private key.
C. The recipient encrypts a message digest with his/her public key.
D. The recipient encrypts a message digest with his/her private key.

Q18 Ah Chong's manager has tasked him with researching an intrusion detection system for a new dispatching center. Ah Chong identifies the top five products and compares their ratings.

Which of the following is the evaluation criteria most in use today for these types of purposes?

A. ITSEC.
B. Common Criteria.
C. Red Book.
D. Orange Book.

Q19 Which one of the following describes the Information Technology Security Evaluation Criteria (ITSEC)?

A. Vendor has the option to define a set of requirements from a menu of possible options into a Security Target (ST).
B. Vendors develop products (Targets of Evaluation, or ToEs) and have them evaluated against the ST.
C. Addresses all three Triad elements.
D. All of the above.

Q20 A cipher that scrambles letters into different positions is referred to as what?

A. Substitution.
B. Stream.
C. Running key.
D. Transposition.

(40 marks)

SECTION B

Q21 (a) Based on Table **Q21**, illustrate the direction of data flow between objects using information flow model.

(8 marks)

TABLE Q21

	A	B	C	D	E
A		X	X		
B	X				X
C		X		X	X
D	X				X
E	X	X			

(b) When most people referring to the Biba model, they are actually referring to the strict integrity model. The strict integrity policy enforces "no write-up" and "no read-down" on the data in the system.

Justify how these strict integrity policies will maintain its integrity.

(4 marks)

(c) State **THREE (3)** Bell-LaPadula policies.

(3 marks)

Q22 Password is a good solution for authenticating the Internet banking system.

(a) Suggest **FOUR (4)** standards to harden the password that could be more secure for Internet banking usage.

(8 marks)

(b) Give **TWO (2)** examples of strong password that employ the password standards suggested in **Q22 (a).**

(2 marks)

Q23 Consider the following scenario.

DataMail wanted to improve their IT disaster recovery capabilities to support their customers and protect critical IT processes. Their first step was to manage their data centers. This allowed them to have data replication across two separate locations with different power and network feeds to protect against power or network outages, and meet the security standards for their clients who serve the financial industry.

With the help of Online Tech, DataMail designed an IT disaster recovery system capable to bring all critical system back online in less than 60 seconds. Hence, the maximum acceptable amount of data loss is only 10 seconds. However, the maximum tolerable amount of time that is needed by DataMail to verify the system and data integrity in less than 40 seconds.

DataMail is hosting their customer-facing systems at Online Tech's Mid-Michigan Data Center and running their disaster recovery servers in the Ann Arbor, Michigan data center 100 kilometres away. The data are replicated between the data centers using Double-Take Software's Double-Take® Availability solution, which provides high availability and failover for physical and virtual servers.

Online Tech provides automatic IP failover that allows the IP addresses of the hosted system to migrate to the second data center should the server or connection to the primary data center fail. Because Online Tech's data centers are interconnected with Gigabit fiber, the failover is nearly instantaneous and does not require DNS reassignment.

Based on the given scenario, answer the following questions:

(a) Calculate the value of Maximum Tolerable Downtime for DataMail.

(5 marks)

(b) What is the Recovery Time Objective (RTO) value?

(2 marks)

(c) Identify type of server backup that DataMail used.

(2 marks)

(d) Justify your answer in **Q23(c).**

(2 marks)

(e) Justify **TWO (2)** reasons why DataMail need to implement Disaster Recovery Plan (DRP).

(4 marks)

Q24 Nurul Aini was appointed as Head of Disaster Recovery Department at ABC Holdings. She need to initiate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for her organization.

(a) Outline **FIVE (5)** phases in implementing BCP and DRP.

(10 marks)

(b) Explain each phases in **Q24 (a)**.

(10 marks)

-END OF QUESTION –