UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2016/2017

COURSE NAME	:	INFORMATION SECURITY STANDARD
COURSE CODE	:	BIS 33203
PROGRAMME CODE	:	3 BIS
EXAMINATION DATE	:	JUNE 2017
DURATION	:	2 HOURS 30 MINUTES
INSTRUCTION	:	ANSWERS **ALL** QUESTIONS

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

SECTION A

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

Q1 Which of the following groups is responsible for project initiation?

A. Functional business units.
B. Senior management.
C. Business Continuity Plan (BCP) team members.
D. Middle management.

Q2 What is the most important aspect of disaster recovery?

A. A complete damage assessment.
B. Control of critical assets.
C. Restoration of business functions.
D. Protection of individual life.

Q3 There is a network printer in the hallway of the company where you work. Many employees do not pick up their printouts immediately and leave them on the printer. What is the consequence of this action to the reliability of the information?

A. The integrity of the information is no longer guaranteed.
B. The availability of the information is no longer guaranteed.
C. The confidentiality of the information is no longer guaranteed.
D. All of the mentioned.

Q4 The purpose of information security policy **BEST** described as _______________.

A. a documentation of the analysis of risks and the search for countermeasures
B. a direction and support to the management regarding information security
C. a concrete security plan by providing with the necessary details
D. an insight into threats and the possible consequences

Q5 ____________ is an example of a human threat.

A. A USB-stick passes on a virus to the network
B. Too much dust in the server room
C. A leak causes a failure of electricity supply
D. An earthquake at 6.5 on the Richter scale

Q6 You received a call from a person claiming to be from the Helpdesk. He asked for your password. What kind of threat is this?

A. Natural threat.
B. Organizational threat.
C. Social Engineering.
D. Phishing.

Q7 Bob had a server crash on Thursday morning. Bob performed a backup in which he used the complete backup from Sunday and several other tapes from Monday, Tuesday, and Wednesday. Which tape-backup method was used?

A. Full restore.
B. Structures restore.
C. Differential restore.
D. Incremental restore.

Q8 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
- possible consequences of the incident

What is the most important information about the incident is missing?

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

Q9 Non repudiation is to ________________.

A. protect against the disclosure of information to unauthorized users
B. protect against a person denying later that a communication or transaction took place
C. assure that a person or system is who or what they claim to be
D. protect against unauthorized changes in data whether intentional or accidental

Q10 A fire breaks out in a branch office of a health insurance company. The personnel are transferred to neighboring branches to continue their work. This happens _______ in the incident cycle.

A. between threat and incident phase
B. between recovery and threat phase
C. between damage and recovery phase
D. between incident and damage phase

Q11 Which **ONE (1)** of the following examples is a threat to integrity?

A. A loose cable.
B. Accidental alteration of data.
C. Private use of data.
D. Outdated anti-virus software.

Q12 _________________ is a preventive measure.

A. Install a logging system that enables changes in a system to be recognized
B. Shut down all Internet traffic after a hacker has gained access to the company systems
C. Put sensitive documents in a safe place
D. Install anti-virus software

Q13 Who is authorized to change the classification of a document?

A. The author of the document.
B. The administrator of the document.
C. The owner of the document.
D. The manager of the owner of the document.

Q14 The computer room is protected by a pass reader. Only the System Management department has a pass. What is the type of security measure used?

A. A corrective security measure.
B. A physical security measure.
C. A logical security measure.
D. A repressive security measure.

Q15 Strong authentication is needed to access highly protected areas. In case of strong authentication, the identity of a person is verified by using three factors. Which factor is verified when we must show our access pass?

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

Q16 Why is it necessary to keep a disaster recovery plan up to date and test it regularly?

A. To have access to recent backups that is located outside the office.
B. To be able to cope with daily occurring faults.
C. To handle event of a far-reaching disruption where the measures taken and the incident procedures planned may not be adequate or may be outdated.
D. To be required by Personal Data Protection legislation.

Q17 You work in the IT department of a medium-sized company. Confidential information has come into the wrong hands several times. This has hurt the image of the company. You have been asked to propose organizational security measures for notebook at your company. What is the first step that you should take?

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

Q18 Establishing whether someone's identity is correct is called _________.

A. authentication
B. authorization
C. identification
D. non repudiation

Q19 A security officer detects that a workstation of an employee is infected with malicious software installed during a phishing attack. Which action is the most beneficial to prevent such incidents in the future?

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

Q20 You are the owner of the courier company MestiKaya. You noticed that the employee use their working time to send and read their private e-mail and surf the Internet. What is the mechanism to permit the usage of the Internet and e-mail facilities legally?

A. Installing an application that makes certain websites no longer accessible and that filters attachments in e-mails.
B. Drafting a code of conduct for the use of the Internet and e-mail in which the rights and obligations of both the employer and staff are set down.
C. Implementing privacy regulations.
D. Installing a virus scanner.

Q21 A cipher that scrambles letters into different positions is referred as _________.

A. substitution
B. stream
C. running key
D. transposition

Q22 Which security model focuses on confidentiality only?

A. Bell-LaPadula.
B. Biba.
C. Clark-Wilson.
D. Biba and Clark-Wilson.

Q23 ____________ is an access system that grants users only those rights necessary for them to perform their work.

A. Discretionary Access
B. Least Privilege
C. Mandatory Access
D. Separation of Duties

Q24 Which **ONE (1)** of the followings is the best description of a digital signature?

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

Q25 ________________ recommends division of responsibilities so that one person cannot commit an undetected fraud.

A. Separation of duties
B. Collusion
C. Need to know
D. Least privilege

(50 marks)

SECTION B

Q26 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 **Q26(a)**.

(2 marks)

Q27 PastiBerjaya Company has four main systems for daily operation that are Operating System, Accounting System, Personel Data and Insurance Data. Ying, Raju and Upin have different roles in the company. The management has provide access to each of them according to their roles. Ying is the IT staff and has full access to Operating System and Accounting System. She can only read the Personel Data but can read and write to Insurance Data. Raju can read and execute the Operating System and Accounting System and can only read Personel Data but does not has access to Insurance Data. Upin can execute and read the Operating System and Accounting System, read the Personel Data but can read and write to Insurance Data.
Note: Read (r), Write (w) and Execute (x).

(a) Draw the Access Control List (ACL) for Ying, Raju and Upin.

(4 marks)

(b) Raju wants to add a module of new accounting calculation to the Accounting System. By considering the Access Control List, who should Raju consults?

(1 marks)

(c) Upin was assigned to recruit new employee for PastiBerjaya Company. Outline suitable process for hiring the new staff.

(5 marks)

Q28 (a) Ramli is to start a job as Head Security Officer at a Pasti Selamat Holding due to the previous officer being fired for incompetence. Note: Imagine he starts on day one with no knowledge of the environment.

Justify Ramli's new job priority as Head of Security Officer.

(5 marks)

(b) Recently, Terus Gemilang Sdn Bhd has gone under attack by Anonymous attacker. You have been appointed as the Chief of Technical Security Officer.

Suggest a high assurance risk management defense to maintain the confidentiality, integrity and availability of data.

(5 marks)

-END OF QUESTIONS –