27

UTHM

Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2018/2019

COURSE NAME	:	INFORMATION SECURITY STANDARD
COURSE CODE	:	BIS 33203
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JUNE / JULY 2019
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

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

TERBUKA

SECTION A

Choose the BEST answer for each of the following questions.

Q1 Resuming critical business functions includes __________.

A. determining the extent of damage
B. declaring a disaster
C. establishing the command center
D. contacting recovery team members

Q2 Which is the **BEST** option if an alternate site is needed to access another network?

A. Secondary Virtual Circuit (SVC).
B. Switched Virtual Circuit (SVC).
C. Temporary Virtual Circuit (TVC).
D. Permanent Virtual Circuit (PVC).

Q3 What is the length of a secret key in the Data Encryption Standard (DES) algorithm?

A. 56-bit.
B. 64-bit.
C. 32-bit.
D. 16-bit.

Q4 A business impact analysis would likely include the following tasks **EXCEPT** _________.

A. calculating risk
B. identifying threats
C. selecting team members
D. identifying critical functions of the company

Q5 Which of the following backup facility is the **LEAST** expensive?

A. Cold.
B. Hot.
C. Warm.
D. Freeze.

TERBUKA

Q6 What is the **BEST** description of a structured walk through test?

A. It is a test to ensure that the critical systems will run at the alternate site.
B. All departments receive a copy of the disaster recovery plan and walk through it.
C. Representatives from each department come together and go through the test collectively.
D. Operations are shifted to the emergency site and senior management reviews the plan on a line item by line item basis.

Q7 What is the **MOST** critical factor in the development of a Disaster Recovery Plan (DRP)?

A. Business Impact Analysis (BIA).
B. Annual testing.
C. Participation from every department.
D. Business Continuity Plan (BCP).

Q8 What is the main reason for using one-way hashing algorithms on user passwords?

A. It provides the compression necessary to conserve hard disk space on the host system.
B. It eliminates the excessive processing required of symmetric encryption.
C. It prevents people from seeing the passwords in clear text.
D. It provides a simplified platform for password for most password cracking utilities.

Q9 What is the **MOST** important factor to consider for an off-site backup facility that will be used to store all backup media?

A. The backup facility should be within 15 minutes of the original facility.
B. The facility should contain an adequate number of PCs and servers and have raised flooring.
C. The facility should have at least one armed guard.
D. The facility should protect against unauthorized access and entry.

Q10 The Common Criteria construct which allows potential consumers or a developer to create standardized sets of security requirements to meet their needs is called __________.

A. a Protection Profile (PP)
B. a Security Target (ST)
C. an evaluation Assurance Level (EAL)
D. a Security Functionality Component Catalog (SFCC)

TERBUKA

Q11 Which of the following **BEST** describe the organization's responsibilities during an unfriendly termination?

A. System access should be removed as quickly as possible after termination.
B. The employee should be given time to remove whatever files he needs from the network.
C. Cryptographic keys can remain the employee's property.
D. Physical removal from the offices would never be necessary.

Q12 Organizations can _________to speed up Redundancy Array of Independent Disk (RAID) access.

A. use larger hard drives
B. stripe the data across several drives
C. mirror critical drives
D. disallow ad hoc queries

Q13 _____________ is used when Advanced Encryption Standard (AES) uses S-boxes during the process of encryption.

A. Substitution
B. Key generation
C. Key exchange
D. Chaining

Q14 Which of the followings **BEST** describe 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.

Q15 You discovered a suspicious document has been stored in a borrowed company's laptop. The document contains sensitive information about your company new product. What is the first action you should take?

A. Delete the document from the laptop to ensure no one else will see it.
B. Contact the author of the document to let him/her know the document was on the laptop.
C. Immediately inform your company's management of your findings and its potential implications.
D. Inform the security awareness trainers that data disclosure prevention in a mobile computing environment needs to be added to their classes.

TERBUKA

Q16 During a disaster or emergency, how does a closed-circuit television (CCTV) help management and security to minimize loss?

A. It helps the management to direct resources to the hardest hit area.
B. It records instances of looting and other criminal activities.
C. It documents shortcomings of plans and procedures.
D. It captures the exposure of assets to physical risk.

Q17 Which of the following is the main goal of a security awareness program?

A. It provides a vehicle for communicating security procedures.
B. It provides a clear understanding of potential risk and exposure.
C. It provides a forum for disclosing exposure and risk analysis.
D. It provides a forum to communicate user responsibilities.

Q18 Which of the following is the **MOST** effective method for reducing security risks associated with building entrances?

A. Minimize the number of entrances.
B. Use solid metal doors and frames.
C. Brightly illuminate the entrances.
D. Install tamperproof hinges and glass.

Q19 What are the assurance designators used in the Common Criteria (CC)?

A. EAL 1, EAL 2, EAL 3, EAL 4, EAL 5, EAL 6, and EAL 7.
B. A1, B1, B2, B3, C2, C1, and D.
C. E0, E1, E2, E3, E4, E5, and E6.
D. AD0, AD1, AD2, AD3, AD4, AD5, and AD6.

Q20 Which of the following is the main goal of Business Continuity Planning (BCP)?

A. Sustain the organization.
B. Recover from a major data center outage.
C. Test the ability to prevent major outages.
D. Satisfy audit requirements.

(40 marks)

TERBUKA

SECTION B

Q21 DataSec wanted to improve their IT disaster recovery capabilities to support their customers and protect critical IT processes. Their first step was to move their servers to separate data center. 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. CompTech help DataSec to design a disaster recovery system that capable to bring all critical system back online in less than 24 hours. The maximum acceptable amount of data loss from the last backup is only 1 hour. DataSec is hosting their customer's systems at CompTech's Data Center and running their disaster recovery servers at data center 100 kilometres away from the DataSec's main office. The data are replicated between the main office and data centers to provide high availability and failover for physical and virtual servers. Moreover, CompTech provides automatic IP failover that allows the IP addresses of the hosted system to migrate to the second data center if the server or connections to the primary data center fail.

Based on the given scenario, answer the following questions:

(a) Calculate the following:

i. Recovery Point Objective (RPO).

ii. Recovery Time Objective (RTO).

iii. Maximum Tolerable Downtime (MTD).

(3 marks)

(b) Identify type of server backup that DataSec used.

(1 mark)

(c) Explain **TWO (2)** benefits of Disaster Recovery Plan (DRP) to DataSec.

(2 marks)

(d) Should DataSec implement restricted asset control towards CompTech access on the IT disaster recovery system? Justify your answer.

(4 marks)

TERBUKA

Q22 You have been asked to design an access control system for a company, called RichMaha Ltd. The company has four sale staff. Three of them are senior staff, S={S1, S2, S3}, and the fourth one is junior staff, J={J1}. The objects to be protected are five file directories, Dir-1, Dir-2, Dir-3, Dir-4 and Dir-5. The access requirement (i.e. policy) is: the senior staffs S1 and S2 have read and write access to Dir-1 and Dir-2 and execute right to Dir-4 and Dir-5. While the senior staff S3 have read access to all files. The junior staffs have read access to Dir-1 and Dir-2, and read and writes access to Dir-3. Draw respective Access Control Matrix tables to illustrate how the above access control requirement are expressed using these models.

(a) Draw the Access Control List (ACL) for the four sale staffs .

(4 marks)

(b) Who should the company consult if they want to make changes to Dir-3 by considering the Access Control List?

(1 mark)

(c) Outline suitable process for hiring new staff in RichMaha Ltd.

(5 marks)

Q23 John was to start a job as Head Security Engineer at a UTHM Holding.

(a) Justify John's job priority as Head of Security Officer.

(10 marks)

(b) Differentiate between policy, standard and procedure.

(6 marks)

(c) Suggest **TWO (2)** policies to access free wireless access for staff and student in UTHM Holding.

(4 marks)

(d) UTHM Holding is at high risk for malware-based attacks. Suggest **THREE (3)** risk management defenses to maintain the confidentiality, integrity and availability to reduce malware infection.

(6 marks)

TERBUKA

Q24 The Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit card records and login data for an undetermined number of user accounts.

In an update on the data breach disclosed earlier this month, Adobe has said that source code for Photoshop was stolen. Making matters worse, a file containing 150 million usernames and hashed passwords has appeared online, and the company says that 38 million accounts were directly impacted by the incident.

Adobe announced that during a security audit in September, the company discovered that attackers had accessed customer names and IDs, encrypted passwords, encrypted credit and debit card numbers, and expiration dates. Adobe also confirmed that source code Adobe Acrobat, ColdFusion, ColdFusion Builder and other Adobe products, was also compromised.

In August 2015, an agreement called for Adobe to pay a $1.1 million in legal fees and an undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices. In November 2016, the amount paid to customers was reported at $1 million.

Based on the given scenario, answer the following questions.

(a) Identify **TWO (2)** assets that Adobe has to protect.

(2 marks)

(b) Identify **TWO (2)** threats for each asset in **Q24(a).**

(4 marks)

(c) Classify **ONE (1)** vulnerability for each threat in **Q24(b).**

(4 marks)

(d) Suggest **ONE (1)** security control that can be use to treat each vulnerability identified in **Q24(c)**. Note: Refer to ISO27001:2013 Reference control objectives and controls document.

(4 marks)

-END OF QUESTIONS –

TERBUKA