

An toan thong tin_ HKII-18-19

Started on	Monday, 1 April 2019, 10:49 AM
State	Finished
Completed on	Monday, 1 April 2019, 11:01 AM
Time taken	11 mins 17 secs
Marks	20.00/20.00
Grade	10.00 out of 10.00 (100%)

Question 1

Correct

Mark 1.00 out of 1.00

What security concept encourages administrators to install firewalls, malware scanners, and an IDS on every host?

Select one:

- ☐ a. Network access control (NAC)
- ☐ b. VLAN
- ☐ c. RADIUS
- ☒ d. Endpoint security

Your answer is correct.

The correct answer is: Endpoint security

Question 2

Correct

Mark 1.00 out of 1.00

Which of the following is a principle of the CIA Triad that means authorized subjects are **granted timely** and uninterrupted access to objects?

Select one:

- ☐ a. Identification
- ☐ b. Layering
- ☒ c. Availability
- ☐ d. Encryption

Your answer is correct.

The correct answer is: Availability

Question 3

Correct

Mark 1.00 out of 1.00

Which one of the following identifies the primary a purpose of information classification processes?

Select one:

- ☐ a. Define the requirements for storing data
- ☐ b. Define the requirements for transmitting data
- ☒ c. Define the requirements for **protecting sensitive data** A primary purpose of information classification processes is to identify security classifications for sensitive data and define the requirements to protect sensitive data. Information classification processes will typically include requirements to protect sensitive data at rest (in backups and stored on media), but not requirements for backing up and storing any data. Similarly, information classification processes will typically include requirements to protect sensitive data in transit, but not any data
- ☐ d. Define the requirements for backing up data

Your answer is correct.

The correct answer is: Define the requirements for protecting sensitive data

Question 4

Correct

Mark 1.00 out of 1.00

Which one of the following data roles is most likely to assign permissions to grant users access to data?

Select one:

- ☒ a. **Administrator** The administrator assigns permissions based on the principles of least privilege and need to know. A custodian protects the integrity and security of the data. Owners have ultimate responsibility for the data and ensure that it is classified properly, and owners provide guidance to administrators on who can have access, but owners do not assign permissions. Users simply access the data
- ☐ b. Custodian
- ☐ c. User
- ☐ d. Owner

Your answer is correct.

The correct answer is: Administrator

Question 5

Correct

Mark 1.00 out of 1.00

If an organization contracts with **outside entities** to provide key business functions or services, such as account or technical support, what is the process called that is used to ensure that these entities support sufficient security?

Select one:

- ☒ a. Third-party governance
- ☐ b. Asset identification
- ☐ c. Qualitative analysis
- ☐ d. Exit interview

Your answer is correct.

The correct answer is: Third-party governance

Question 6

Correct

Mark 1.00 out of 1.00

What ensures that the subject of an activity or event **cannot deny** that the event occurred?

Select one:

- ☐ a. CIA Triad
- ☐ b. Hash totals
- ☐ c. Abstraction
- ☒ d. Nonrepudiation Nonrepudiation ensures that the subject of an activity or event cannot deny that the event occurred.

Your answer is correct.

The correct answer is: Nonrepudiation

Question 7

Correct

Mark 1.00 out of 1.00

Which of the following contains the primary goals and objectives of security?

Select one:

- ☐ a. A stand-alone system
- ☐ b. A network's border perimeter
- ☒ c. The CIA Triad
- ☐ d. The Internet

Your answer is correct.

The correct answer is: The CIA Triad

Question 8

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☒ a. Humans
- ☐ b. Internet connections
- ☐ c. Software products
- ☐ d. Security policies

Your answer is correct.

The correct answer is: Humans

Question 9

Correct

Mark 1.00 out of 1.00

Which one of the following would administrators use to **connect to a remote server securely** for administration?

Select one:

- ☐ a. Telnet
- ☐ b. Secure Copy (SCP)
- ☒ c. Secure Shell (SSH) SSH is a secure alternative to Telnet because it encrypts data transmitted over a network. In contrast, Telnet transmits data in cleartext. SFTP and SCP are good methods for transmitting sensitive data over a network, but not for administration purposes.
- ☐ d. Secure File Transfer Protocol (SFTP)

Your answer is correct.

The correct answer is: Secure Shell (SSH)

Question 10

Correct

Mark 1.00 out of 1.00

Which networking technology is based on the IEEE 802.3 standard?

Select one:

- ☐ a. HDLC
- ☐ b. FDDI
- ☒ c. Ethernet
- ☐ d. Token Ring

Your answer is correct.

The correct answer is: Ethernet

Question 11

Correct

Mark 1.00 out of 1.00

What is encapsulation?

Select one:

- ☒ a. Adding a header and footer to data as it moves down the OSI stack
- ☐ b. Protecting evidence until it has been properly collected
- ☐ c. Changing the source and destination addresses of a packet
- ☐ d. Verifying a person's identity

Your answer is correct.

The correct answer is: Adding a header and footer to data as it moves down the OSI stack

Question 12

Correct

Mark 1.00 out of 1.00

Vulnerabilities and risks are evaluated based on their threats against which of the following?

Select one:

- ☒ a. One or more of the CIA Triad principles
- ☐ b. Due care
- ☐ c. Data usefulness
- ☐ d. Extent of liability

Your answer is correct.

The correct answer is: One or more of the CIA Triad principles

Question 13

Correct

Mark 1.00 out of 1.00

Which of the following is not considered a violation of confidentiality?

Select one:

- ☐ a. Stealing passwords
- ☐ b. Social engineering
- ☒ c. Hardware destruction
- ☐ d. Eavesdropping

Your answer is correct.

The correct answer is: Hardware destruction

Question 14

Correct

Mark 1.00 out of 1.00

If a security mechanism offers availability, then it offers a high level of assurance that authorized subjects can _____ the data, objects, and resources.

Select one:

- ☒ a. Access
- ☐ b. Repudiate
- ☐ c. Control
- ☐ d. Audit

Your answer is correct.

The correct answer is: Access

Question 15

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☐ a. Vulnerability assessment
- ☐ b. Business continuity plan
- ☒ c. Disaster recovery plan Disaster recovery plans pick up where business continuity plans leave off. After a disaster strikes and the business is interrupted, the disaster recovery plan guides response teams in their efforts to quickly restore business operations to normal levels.
- ☐ d. Business impact assessment

Your answer is correct.

The correct answer is: Disaster recovery plan

Question 16

Correct

Mark 1.00 out of 1.00

What is the first step that individuals responsible for the development of a business continuity plan should perform?

Select one:

- ☒ a. Business organization analysis The business organization analysis helps the initial planners select appropriate BCP team members and then guides the overall BCP process
- ☐ b. Resource requirements analysis
- ☐ c. BCP team selection
- ☐ d. Legal and regulatory assessment

Your answer is correct.

The correct answer is: Business organization analysis

Question 17

Correct

Mark 1.00 out of 1.00

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

Select one:

- ☐ a. Wait until you and the employee are the only people remaining in the building before announcing the termination
- ☒ b. Disable the employee's network access just as they are informed of the termination You should remove or disable the employee's network user account immediately before or at the same time they are informed of their termination.
- ☐ c. Inform the employee a few hours before they are officially terminated.
- ☐ d. Send out a broadcast email informing everyone that a specific employee is to be terminated.

Your answer is correct.

The correct answer is: Disable the employee's network access just as they are informed of the termination

Question 18

Correct

Mark 1.00 out of 1.00

When seeking to hire new employees, what is the first step?

Select one:

- ☐ a. Screen candidates
- ☐ b. Request resumes
- ☐ c. Set position classification
- ☒ d. Create a job description The first step in hiring new employees is to create a job description. Without a job description, there is no consensus on what type of individual needs to be found and hired.

Your answer is correct.

The correct answer is: Create a job description

Question 19

Correct

Mark 1.00 out of 1.00

What security control is directly focused on preventing collusion?

Select one:

- ☐ a. Job descriptions
- ☒ b. Separation of duties The likelihood that a co-worker will be willing to collaborate on an illegal or abusive scheme is reduced because of the higher risk of detection created by the combination of separation of duties, restricted job responsibilities, and job rotation
- ☐ c. Principle of least privilege
- ☐ d. Qualitative risk analysis

Your answer is correct.

The correct answer is: Separation of duties

Question 20

Correct

Mark 1.00 out of
1.00

Which of the following is the most important aspect of security?

Select one:

- ☐ a. Logical security
- ☐ b. Awareness training
- ☒ c. Physical security Physical security is the most important aspect of overall security. Without physical security, none of the other aspects of security are sufficient
- ☐ d. Intrusion detection

Your answer is correct.

The correct answer is: Physical security

◀ Chapter 1 - Computer Security Concepts

Chapter 2 - Cryptography ▶

Return to: Chapter 1 - Com... ➡