Fundamentals of Information Systems Security 5th edition Kim Test Bank

SKU: 9781284314977-TEST-BANK

Chapter 1

Multiple Choice

1. Which term describes any action that could damage an asset?
   A) Risk
   B) Countermeasure
   C) Vulnerability
   D) Threat

Ans: D
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy: Remember

2. Which of the following is a non-U.S. regulation?
   A) Health Insurance Portability and Accountability Act (HIPAA)
   B) Protection of Personal Information (APPI)
   C) Children's Internet Protection Act (CIPA)
   D) Gramm-Leach-Bliley Act (GLBA)

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

3. A healthcare worker accesses a patient's electronic medical records without a valid reason. The worker is not involved in the patient's care and does not have proper authorization to view this information. Which of the tenets of information security was violated?
   A) Confidentiality
   B) Integrity
   C) Availability
   D) Nonrepudiation

Ans: A

Fundamentals of Information Systems Security 5th edition Kim Test Bank

H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Apply

4. What is the amount of time it takes to recover and make a system, application, and data available for use after an outage?
   A) Recovery point objective (RPO)
   B) Mean time to failure (MTTF)
   C) Mean time to repair (MTTR)
   D) Recovery time objective (RTO)

Ans: D
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

5. Bob's web server was down for two days in January. It experienced no other downtime during that month. What represents the web server uptime for that month?
   A) 96.67%
   B) 93.55%
   C) 99.96%
   D) 1.069%

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Hard
Taxonomy: Analyze

6. Which domain of a typical IT infrastructure is the first layer of defense for a layered security strategy?
   A) User Domain
   B) Workstation Domain
   C) System/Application Domain
   D) LAN Domain

Ans: A
H1-head: Information Systems Security

Fundamentals of Information Systems Security 5th edition Kim Test Bank

Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

7. Which security control is most helpful in protecting against eavesdropping on wireless local area network (WLAN) data transmissions to maintain confidentiality?
   A) Defining server, desktop, and laptop vulnerability window policies, standards, procedures, and guidelines
   B) Deploying an intrusion detection system/intrusion prevention system (IDS/IPS)
   C) Making wiring closets physically secure
   D) Implementing encryption between workstations and wireless access points (WAPs)

Ans: D
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

8. Devaki is capturing traffic on her network. She notices connections using ports 20, 22, 23, and 80. Which port normally hosts a protocol that uses secure, encrypted connections?
   A) 20
   B) 22
   C) 23
   D) 80

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Hard
Taxonomy: Understand

9. Which network device is designed to block network connections that are identified as potentially malicious?
   A) Intrusion detection system (IDS)
   B) Intrusion prevention system (IPS)
   C) Router
   D) Web server

Fundamentals of Information Systems Security 5th edition Kim Test Bank

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

10. Which risk is most effectively mitigated by an upstream Internet service provider (ISP)?
    A) Distributed denial of service (DDoS)
    B) Inherently insecure Transmission Control Protocol/Internet Protocol (TCP/IP) applications
    C) Firewall configuration error
    D) Unauthorized remote access

Ans: A
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Hard
Taxonomy: Analyze

11. Which domain of an IT infrastructure is described as a collection of computers and devices connected to one another or to a common connection medium, which can include wires, fiber-optic cables, or radio waves. The domain is generally organized by function or department.
    A) Workstation Domain
    B) LAN Domain
    C) Remote Access Domain
    D) System/Application Domain

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

12. What is a primary risk to the Workstation Domain, the LAN Domain, and the System/Application Domain?
    A) Unauthorized access to systems
    B) Unauthorized network probing and port scanning

Fundamentals of Information Systems Security 5th edition Kim Test Bank

C) Mobile worker token or other authentication stolen
D) Downtime of IT systems for an extended period after a disaster

Ans: A
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

13. Which domain of a typical IT infrastructure is where all data travels into and out of the IT infrastructure and where Internet access is provided for the entire organization?
A) WAN Domain
B) System/Application Domain
C) Remote Access Domain
D) LAN-to-WAN Domain

Ans: D
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

14. Remote access security controls help to ensure that the user connecting to an organization's network is who the user claims to be. A username is commonly used for _____, whereas a biometric scan could be used for _____.
A) identification, authorization
B) identification, authentication
C) authorization, accountability
D) authentication, authorization

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Analyze

15. Maria is writing a policy that defines a priority for mission-critical IT systems and data. The policy is aligned with the organization's business impact analysis (BIA)

Fundamentals of Information Systems Security 5th edition Kim Test Bank

and is used to address risks that could threaten the organization's ability to continue operations after a disaster. Which policy is Maria writing?
A) Asset protection policy
B) Information asset classification policy
C) Continuous monitoring policy
D) Asset management policy

Ans: A
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Hard
Taxonomy: Understand

16. Which element of the security policy framework comes from upper management and applies to the entire organization?
A) Policy
B) Standard
C) Guideline
D) Procedure

Ans: A
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy: Remember

17. Which element of the security policy framework offers suggestions rather than mandatory actions?
A) Policy
B) Standard
C) Guideline
D) Procedure

Ans: C
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Understand

Fundamentals of Information Systems Security 5th edition Kim Test Bank

18. Chris is writing a document that provides step-by-step instructions for end users seeking to update the security software on their computers. Performing these updates is mandatory. Which type of document is Chris writing?
    A) Policy
    B) Standard
    C) Guideline
    D) Procedure

Ans: D
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy: Apply

19. Which element of the IT security policy framework provides detailed written definitions for hardware and software and how they are to be used?
    A) Policy
    B) Standard
    C) Guideline
    D) Procedure

Ans: B
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy: Remember

20. Carrie is creating a data classification standard for her company. Which data classification should she assign to information, such as solution briefs and white papers, that will be shared openly on the company's website?
    A) Private
    B) Confidential
    C) Internal Use Only
    D) Public-domain data

Ans: D
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy: Apply

Fundamentals of Information Systems Security 5th edition Kim Test Bank

True/False

1. True or False? The General Data Protection Regulation (GDPR) is a Japanese regulation that specifies how companies and business are to handle the private information of Japanese residents.

Ans: False
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

2. True or False? A communications protocol is a list of rules and methods for communicating across the Internet.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

3. True or False? The protocols in the Transmission Control Protocol/Internet Protocol (TCP/IP) suite work together to allow any two computers to be connected and thus create a network.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

4. True or False? An information system is a safeguard or countermeasure an organization implements to help reduce risk.

Ans: False
H1-head: Information Systems Security

Fundamentals of Information Systems Security 5th edition Kim Test Bank

Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

5. True or False? Availability is the tenet of information security that deals with uptime and downtime.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

6. True or False? Generative AI applications can mimic human-to-human dialogue.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

7. True or False? An IT security policy framework consists of policies, standards, procedures, and guidelines that reduce risks and threats.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

8. True or False? Hypertext Transfer Protocol (HTTP) is the communications protocol between web browsers and websites with data in cleartext.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy

Fundamentals of Information Systems Security 5th edition Kim Test Bank

Taxonomy:

9. True or False? Downtime is the total amount of time that a system, application, and data are not accessible.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

10. True or False? Service-level agreements (SLAs) are a common part of the User Domain of a typical IT infrastructure.

Ans: False
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

11. True or False? Networks, routers, and equipment require continuous monitoring and management to keep wide area network (WAN) service available.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

12. True or False? An intrusion detection system (IDS) is a security appliance that is used to filter Internet Protocol (IP) packets and block unwanted packets.

Ans: False
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Hard
Taxonomy:

Fundamentals of Information Systems Security 5th edition Kim Test Bank

13. True or False? The LAN-to-WAN Domain is where the IT infrastructure links to a WAN and the Internet.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

14. True or False? The LAN Domain of a typical IT infrastructure includes both physical network components and logical configuration of services for users.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

15. True or False? Hypertext Transfer Protocol (HTTP) encrypts data transfers between secure browsers and secure webpages.

Ans: False
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

16. True or False? Authorization is the process of granting rights to use an organization's IT assets, systems, applications, and data to a specific user.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

Fundamentals of Information Systems Security 5th edition Kim Test Bank

17. True or False? The System/Application Domain of a typical IT infrastructure consists of hardware, operating system software, applications, and data, and it includes hardware and its logical design.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

18. True or False? The User Domain of a typical IT infrastructure defines the people and processes that access an organization's information systems.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

19. True or False? Encrypting data within databases and storage devices gives an added layer of security.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Easy
Taxonomy:

20. True or False? A data classification standard provides a consistent definition for how an organization should handle and secure different types of data.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

Fundamentals of Information Systems Security 5th edition Kim Test Bank

21. True or False? For businesses and organizations under recent compliance laws, data classification standards typically include private, confidential, internal use only, and public-domain categories.

Ans: True
H1-head: Information Systems Security
Subject: Chapter 1
Title: Information Systems Security
Complexity: Medium
Taxonomy:

Fundamentals of Information Systems Security 5th edition Kim Test Bank