Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

SKU: 9780357508329-TEST-BANK

Name:_____ Class:_____ Date:_____

Module 01 - An Overview of Information Security and Risk Management

True / False

1. The C.I.A. triad is the industry standard for computer security since the development of the mainframe and is based on three characteristics that describe the utility of information.

a. True
b. False

ANSWER: True
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
p. 3
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 12:38 PM
DATE MODIFIED: 12/27/2020 10:41 AM

2. Confidentiality is an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

a. True
b. False

ANSWER: True
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 12:45 PM
DATE MODIFIED: 7/25/2020 2:49 PM

3. A power spike is a long-term increase in electrical power availability.

a. True
b. False

ANSWER: False
POINTS: 1
REFERENCES: p. 6
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 12:53 PM
DATE MODIFIED: 12/27/2020 10:42 AM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

4. Intellectual property (IP) includes trade secrets, copyrights, trademarks, and patents.

a. True

b. False

ANSWER: True
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
p. 6
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 5/7/2020 4:06 PM
DATE MODIFIED: 12/27/2020 10:43 AM

5. A hacker is an information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

a. True

b. False

ANSWER: False
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
p. 7
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:28 PM
DATE MODIFIED: 12/27/2020 10:45 AM

6. A disaster recovery plan (DR plan) deals with identifying, classifying, responding to, and recovering from an incident.

a. True

b. False

ANSWER: False
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
p. 37
QUESTION TYPE: True / False
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 5/7/2020 4:06 PM
DATE MODIFIED: 12/27/2020 10:48 AM

Modified True / False

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

7. Confidentiality is the state of being secure and free from danger or harm.

ANSWER: False - Security
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
p. 2
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 12:42 PM
DATE MODIFIED: 12/27/2020 10:49 AM

8. Integrity is an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

ANSWER: False - Confidentiality
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 12:48 PM
DATE MODIFIED: 12/27/2020 10:50 AM

9. Noise is the presence of additional and disruptive signals in network communications or electrical power delivery.

ANSWER: True
POINTS: 1
REFERENCES: p. 6
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 12:54 PM
DATE MODIFIED: 7/25/2020 3:33 PM

10. A penetration tester is someone who conducts attacks for personal financial benefit or for a crime organization or foreign government.

ANSWER: False - professional hacker
POINTS: 1
REFERENCES: p. 7
H1: AN OVERVIEW OF INFORMATION SECURITY

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:30 PM
DATE MODIFIED: 7/25/2020 3:37 PM

11. A rainbow table is a list of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.
ANSWER: True
POINTS: 1
REFERENCES: p. 8
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:32 PM
DATE MODIFIED: 7/25/2020 3:39 PM

12. Pretexting is when an attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.
ANSWER: False - Phishing
POINTS: 1
REFERENCES: p. 9
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:33 PM
DATE MODIFIED: 12/27/2020 10:50 AM

13. A worm is a type of malware that is attached to other executable programs.
ANSWER: False - virus
POINTS: 1
REFERENCES: p. 10
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:36 PM
DATE MODIFIED: 7/25/2020 3:44 PM

14. Cyberterrorism is the conduct of terrorist activities by online attackers.
ANSWER: True
POINTS: 1
REFERENCES: p. 10
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:37 PM
DATE MODIFIED: 7/25/2020 3:46 PM

15. A denial of service is a malware payload that provides access to a system by bypassing normal access controls.
ANSWER: False - back door
POINTS: 1
REFERENCES: p. 11
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:39 PM
DATE MODIFIED: 12/27/2020 10:51 AM

16. Policies are nonmandatory recommendations the employee may use as a reference in complying with directives.
ANSWER: False - Guidelines
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
p. 13
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/20/2020 5:39 PM
DATE MODIFIED: 12/27/2020 10:52 AM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

17. Issue-specific security policy is an organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resource, such as one of its processes or technologies.

ANSWER: True
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Types of InfoSec Policies
p. 14
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/20/2020 5:40 PM
DATE MODIFIED: 12/27/2020 10:53 AM

18. Policies are living documents that must be nurtured, given that they are constantly changing and growing.

ANSWER: True
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Guidelines for Effective Policy Development and Implementation
p. 18
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/20/2020 5:42 PM
DATE MODIFIED: 12/27/2020 10:54 AM

19. The RM framework is the identification, analysis, evaluation, and treatment of risk to information assets, as specified in the RM methodology.

ANSWER: False - RM process
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
p. 20
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 5:43 PM
DATE MODIFIED: 12/27/2020 10:55 AM

20. Risk treatment is the selection of a strategy to address residual risk in an effort to bring it into alignment with

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

the organization's risk appetite.

ANSWER: True
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
p. 21
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 5:46 PM
DATE MODIFIED: 7/25/2020 4:09 PM

21. Risk appetite is the recognition, enumeration, and documentation of risks to an organization's information assets.

ANSWER: False - identification
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
p. 24
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 5:51 PM
DATE MODIFIED: 7/25/2020 4:11 PM

22. Risk analysis is the probability that a specific vulnerability within an organization will be attacked by a threat.

ANSWER: False - Likelihood
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
p. 30
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 5:54 PM
DATE MODIFIED: 7/25/2020 4:14 PM

23. The transference risk treatment strategy attempts to shift risk to other assets, other processes, or other organizations.

ANSWER: True
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

p. 36
QUESTION TYPE: Modified True / False
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 5:56 PM
DATE MODIFIED: 7/25/2020 4:16 PM

Multiple Choice

24. The entire program of planning for and managing risk to information assets in the organization is referred to as _____.
a. risk management
b. information security
c. contingency planning
d. loss control

ANSWER: a
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
p. 2
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 1:48 PM
DATE MODIFIED: 7/26/2020 2:20 PM

25. ____ ensures that only those with the rights and privileges to access information are able to do so.
a. Confidentiality
b. Availability
c. Integrity
d. Risk assessment

ANSWER: a
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 4/29/2020 11:05 AM
DATE MODIFIED: 7/26/2020 2:28 PM

26. Information assets have ____ when authorized users -- people or computer systems -- are able to access them in the specified format without interference or obstruction.
a. integrity
b. availability

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

c. confidentiality
d. risk assessment

ANSWER: b
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 4/29/2020 10:47 AM
DATE MODIFIED: 12/27/2020 11:05 AM

27. _____ is the protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.
a. Risk management
b. Information security
c. Contingency planning
d. Loss control

ANSWER: b
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 1:50 PM
DATE MODIFIED: 12/27/2020 11:05 AM

28. Information assets have ____ when they are not exposed (while being stored, processed, or transmitted) to corruption, damage, destruction, or other disruption of their authentic states.
a. risk assessment
b. availability
c. integrity
d. confidentiality

ANSWER: c
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 4/29/2020 11:14 AM
DATE MODIFIED: 7/26/2020 2:34 PM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

29. A subject or object's ability to use, manipulate, modify, or affect another subject or object is known as _____.
    a. access
    b. exposure
    c. risk
    d. vulnerability

ANSWER: a
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: Key Information Security Concepts
p. 34
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 1:53 PM
DATE MODIFIED: 7/26/2020 2:37 PM

30. A potential weakness in an asset or its defensive control system(s) is known as _____.
    a. access
    b. exposure
    c. risk
    d. vulnerability

ANSWER: d
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: Key Information Security Concepts
p. 5
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 1:55 PM
DATE MODIFIED: 7/26/2020 2:38 PM

31. A(n) ____ is any event or circumstance that has the potential to adversely affect operations and assets.
    a. payload
    b. intellectual property
    c. Trojan horse
    d. threat

ANSWER: d
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: Key Information Security Concepts
p. 5
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 1:57 PM
DATE MODIFIED: 7/26/2020 2:40 PM

32. ____ is the presence of additional and disruptive signals in network communications or electrical power delivery.
a. Payload
b. Noise
c. Fault
d. Threat

ANSWER: b
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
p. 6
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 4/29/2020 10:59 AM
DATE MODIFIED: 12/27/2020 11:08 AM

33. A(n) ____ is a short-term increases in electrical power availability, also known as a swell.
a. spike
b. noise
c. fault
d. threat

ANSWER: a
POINTS: 1
REFERENCES: p. 6
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 2:02 PM
DATE MODIFIED: 12/27/2020 11:09 AM

34. The term ____ refers to a broad category of electronic and human activities in which an unauthorized individual gains access to the information an organization is trying to protect.
a. theft
b. trespass
c. polymorphism
d. denial of service

ANSWER: b
POINTS: 1

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

REFERENCES: p. 7
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 5/18/2020 3:49 PM
DATE MODIFIED: 12/27/2020 11:10 AM

35. A ___ attack attempts to narrow the range of possible passwords by using a list of common passwords and possibly including attempts based on the target's personal information.

a. brute force password
b. rainbow table
c. dictionary password
d. dictionary table

ANSWER: c
POINTS: 1
REFERENCES: p. 8
H2: The 12 Categories of Threats
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 2:04 PM
DATE MODIFIED: 7/26/2020 2:56 PM

36. _____ is a form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information; it is commonly performed by telephone.

a. Phishing
b. Advance-fee fraud (AFF)
c. Pretexting
d. Ransomware

ANSWER: c
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
p. 9
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 4:23 PM
DATE MODIFIED: 12/27/2020 11:11 AM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

37. _____ is a form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail) that contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

a. Phishing
b. Advance-fee fraud (AFF)
c. Pretexting
d. Ransomware

ANSWER: a
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
p. 9
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/21/2020 2:08 PM
DATE MODIFIED: 12/27/2020 11:12 AM

38. ____ involves the hacking of systems to conduct terrorist activities against systems or networks.

a. Cyberterrorism
b. Script hacking
c. Program overflow
d. Social engineering

ANSWER: a
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
p. 10
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 4/29/2020 11:01 AM
DATE MODIFIED: 7/26/2020 3:00 PM

39. A _____ is a type of malware that is capable of activation and replication without being attached to an existing program.

a. virus
b. worm
c. zombie
d. pharm

ANSWER: b
POINTS: 1
REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

	p. 10
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	1.1 - Define and explain information security
DATE CREATED:	7/21/2020 4:28 PM
DATE MODIFIED:	7/26/2020 3:04 PM

40. A ____ attack seeks to deny legitimate users access to services by either tying up a server's available resources or causing it to shut down.

a. Trojan horse
b. DoS
c. social engineering
d. spyware

ANSWER:	b
POINTS:	1
REFERENCES:	H1: AN OVERVIEW OF INFORMATION SECURITY H2: The 12 Categories of Threats p. 11
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	1.1 - Define and explain information security
DATE CREATED:	4/29/2020 10:50 AM
DATE MODIFIED:	7/26/2020 3:07 PM

41. A _____ is a type of malware that is attached to other executable programs; when activated, it replicates and propagates to multiple systems, spreading by multiple communications vectors.

a. virus
b. worm
c. zombie
d. bot

ANSWER:	a
POINTS:	1
REFERENCES:	H1: AN OVERVIEW OF INFORMATION SECURITY H2: The 12 Categories of Threats p. 10
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	1.1 - Define and explain information security
DATE CREATED:	7/21/2020 4:26 PM
DATE MODIFIED:	12/27/2020 11:15 AM

42. A(n) ____ represents a formal statement of the organization's managerial philosophy.

a. policy
b. procedure

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

c. standard
d. guideline

ANSWER: a
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
p. 12
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 4/29/2020 11:16 AM
DATE MODIFIED: 7/26/2020 3:12 PM

43. A(n) ____ represents nonmandatory recommendations the employee may use as a reference in complying with the policy.
a. practice
b. procedure
c. standard
d. guideline

ANSWER: d
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Key Policy Components
p. 13
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:33 PM
DATE MODIFIED: 7/26/2020 3:16 PM

44. A(n) ____ represents an example of actions that illustrate compliance with policies.
a. practice
b. procedure
c. standard
d. guideline

ANSWER: a
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Key Policy Components
p. 13
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:32 PM
DATE MODIFIED: 7/26/2020 3:18 PM

45. A(n) _____ security policy addresses specific areas of technology and contains a statement about the organization's position on a specific issue.

a. issue-specific
b. enterprise information
c. systems-specific
d. technology-specific

ANSWER: a
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Types of InfoSec Policies
p. 14
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:35 PM
DATE MODIFIED: 12/27/2020 11:18 AM

46. A(n) _____ security policy often may function as standards or procedures to be used when configuring or maintaining technical infrastructure.

a. issue-specific
b. enterprise information
c. systems-specific
d. technology-specific

ANSWER: c
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Types of InfoSec Policies
p. 15
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:38 PM
DATE MODIFIED: 12/27/2020 11:19 AM

47. Which of the following represents the proper sequence for policy development?

a. Policy is designed and written, policy is reviewed and formally approved, and the policy is perpetuated within the organization
b. Policy is reviewed and formally approved, the policy is perpetuated within the organization, and policy is designed and written

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

c. The policy is perpetuated within the organization, policy is designed and written, and policy is reviewed and formally approved

d. Policy is designed and written, the policy is perpetuated within the organization, and policy is reviewed and formally approved

ANSWER: a
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Guidelines for Effective Policy Development and Implementation
p. 16
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:41 PM
DATE MODIFIED: 12/27/2020 11:21 AM

48. Policy compliance means the employee _____.

a. must agree to the policy

b. must have read the policy

c. should follow the policy

d. has the option to comply with the policy

ANSWER: a
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Guidelines for Effective Policy Development and Implementation
p. 17
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:47 PM
DATE MODIFIED: 7/26/2020 3:29 PM

49. To remain viable, security policies must have all of the following EXCEPT _____.

a. an individual responsible for the creation, revision, distribution, and storage of the policy

b. a schedule of reviews to ensure currency and accuracy, and to demonstrate due diligence

c. a mechanism by which individuals can comfortably make recommendations for revisions, preferably anonymously

d. the use of a policy management software package to streamline the steps in creating and managing policy

ANSWER: d
POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Guidelines for Effective Policy Development and Implementation
p. 18

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/21/2020 4:51 PM
DATE MODIFIED: 12/27/2020 11:22 AM

50. _____ is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components of those systems.

a. Information security
b. Contingency planning
c. Security management
d. Risk management

ANSWER: d
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
p. 19
H2: Knowing Yourself and Knowing Your Enemy
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 4:55 PM
DATE MODIFIED: 12/27/2020 5:58 PM

51. It is essential that all stakeholders conduct periodic asset inventories. Which of the following is not part of this essential activity that must be periodically performed?

a. Verify the completeness and accuracy of the asset inventory.
b. Review and verify the threats and vulnerabilities that have been identified as dangerous to the asset inventory.
c. Regularly verify the ongoing effectiveness of every control that's been deployed.
d. Certify that no cybersecurity losses have occurred.

ANSWER: d
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Knowing Yourself and Knowing Your Enemy
p. 20
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 4:58 PM
DATE MODIFIED: 12/27/2020 5:59 PM

52. Risk ____ is an approach to combining risk identification, risk analysis, and risk evaluation into a single strategy.

a. treatment
b. assessment
c. resolution

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

d. aversion

ANSWER: b
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
p. 21
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 4/29/2020 10:58 AM
DATE MODIFIED: 7/27/2020 3:39 PM

53. Risk ____ is the selection of a strategy to address residual risk in an effort to bring it into alignment with the organization's risk appetite.

a. treatment
b. assessment
c. resolution
d. aversion

ANSWER: a
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
p. 21
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 5:06 PM
DATE MODIFIED: 12/27/2020 6:00 PM

54. Which of the following describes the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-off between perfect security and unlimited accessibility?

a. risk appetite
b. risk tolerance
c. residual risk
d. risk threshold

ANSWER: a
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
p. 22
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 5:10 PM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

DATE MODIFIED: 12/27/2020 6:02 PM

55. The risk to information assets that remains even after current controls have been applied is known as _____.

a. risk appetite
b. risk tolerance
c. residual risk
d. risk threshold

ANSWER: c
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
p. 22
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 5:08 PM
DATE MODIFIED: 7/27/2020 4:40 PM

56. ____ is the process of recognizing and documenting the organization's information technology and the risks it faces.

a. Risk identification
b. Data classification
c. Security risk review
d. Risk tolerance

ANSWER: a
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
p. 24
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 4/29/2020 11:13 AM
DATE MODIFIED: 7/27/2020 4:43 PM

57. A formal access control methodology used to assign a level of confidentiality to an information asset and thus restrict the number of people who can access it is known as a(n) _____.

a. data classification scheme
b. asset categorization model
c. data priority scheme
d. access control list

ANSWER: a
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

	p. 26
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED:	7/21/2020 5:13 PM
DATE MODIFIED:	7/27/2020 4:44 PM

58. As each information asset is identified, categorized, and _____, a relative value must be assigned to it to enable comparative judgments intended to ensure that the most valuable information assets are given the highest priority when managing risk.

a. labeled
b. prioritized
c. classified
d. ranked

ANSWER:	c
POINTS:	1
REFERENCES:	H1: OVERVIEW OF RISK MANAGEMENT H2: The RM Process p. 27
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED:	7/21/2020 5:15 PM
DATE MODIFIED:	7/27/2020 4:48 PM

59. An understanding of the potential consequences of a successful attack on an information asset by a threat is known in the risk analysis process as _____.

a. impact
b. opportunity
c. likelihood
d. severity

ANSWER:	a
POINTS:	1
REFERENCES:	H1: OVERVIEW OF RISK MANAGEMENT H2: The RM Process p.30
QUESTION TYPE:	Multiple Choice
HAS VARIABLES:	False
LEARNING OBJECTIVES:	1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED:	7/21/2020 5:26 PM
DATE MODIFIED:	12/27/2020 6:40 PM

60. ____ is a process of comparing an information asset's risk rating to the numerical representation of the organization's risk appetite or risk threshold to determine if risk treatment is required.

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

a. Risk control
b. Risk evaluation
c. Risk determination
d. Risk avoidance

ANSWER: b
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
p. 34
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 5/18/2020 5:22 PM
DATE MODIFIED: 12/27/2020 6:43 PM

61. ____ is the risk control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

a. Avoidance
b. Transference
c. Acceptance
d. Mitigation

ANSWER: d
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
p. 37
QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 4/29/2020 10:55 AM
DATE MODIFIED: 7/27/2020 5:36 PM

62. ____ is a risk treatment strategy that attempts to eliminate or reduce any remaining uncontrolled risk through the application of additional controls and safeguards in an effort to change the likelihood of a successful attack on an information asset.

a. Transference
b. Mitigation
c. Acceptance
d. Defense

ANSWER: d
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
p. 36

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

QUESTION TYPE: Multiple Choice
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/21/2020 5:33 PM
DATE MODIFIED: 7/27/2020 5:38 PM

Completion

63. The _____ attribute of information describes how data is accessible and correctly formatted for use without interference or obstruction.
ANSWER: availability
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:43 PM
DATE MODIFIED: 7/28/2020 3:11 PM

64. _____ is defined by the Committee on National Security Systems (CNSS) as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.
ANSWER: Information security
POINTS: 1
REFERENCES: p. 3
H1: AN OVERVIEW OF INFORMATION SECURITY
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 5/19/2020 11:12 AM
DATE MODIFIED: 7/28/2020 3:12 PM

65. The probability of an unwanted occurrence, such as an adverse event or loss, is known as _____.
ANSWER: risk
POINTS: 1
REFERENCES: p. 4
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: Key Information Security Concepts
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

DATE CREATED: 7/20/2020 3:45 PM
DATE MODIFIED: 12/27/2020 6:47 PM

66. A potential weakness in an asset or its defensive control systems is known as a _____.
ANSWER: vulnerability
POINTS: 1
REFERENCES: p. 5
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: Key Information Security Concepts
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:47 PM
DATE MODIFIED: 12/27/2020 6:47 PM

67. The unauthorized duplication, installation, or distribution of copyrighted computer software is known as _____.
ANSWER: software piracy
POINTS: 1
REFERENCES: p. 6
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:48 PM
DATE MODIFIED: 7/28/2020 3:19 PM

68. A person who accesses systems and information without authorization and often illegally is known as a(n) _____.
ANSWER: hacker
POINTS: 1
REFERENCES: p. 7
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:51 PM
DATE MODIFIED: 7/28/2020 3:20 PM

69. A _____ password attack is an attempt to guess a password by trying every possible combination of characters and numbers in it.

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

ANSWER: brute force
POINTS: 1
REFERENCES: p. 8
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:52 PM
DATE MODIFIED: 7/28/2020 3:21 PM

70. The process of _____ uses interpersonal skills to convince people to reveal access credentials or other valuable information to an attacker.
ANSWER: social engineering
POINTS: 1
REFERENCES: p. 9
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:53 PM
DATE MODIFIED: 7/28/2020 3:22 PM

71. Computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption is known as _____.
ANSWER: ransomware
POINTS: 1
REFERENCES: p. 9
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:55 PM
DATE MODIFIED: 7/28/2020 3:26 PM

72. _____ is a spear-phishing and blackmail attack that demands payment to preclude the distribution of hacked recordings of the target visiting pornographic Web sites.
ANSWER: Sextortion
POINTS: 1

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

REFERENCES: p. 10
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:58 PM
DATE MODIFIED: 8/1/2020 5:00 PM

73. The types of malware that are capable of activation and replication without being attached to an existing program are called _____.
ANSWER: worms
POINTS: 1
REFERENCES: p. 10
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 3:59 PM
DATE MODIFIED: 7/28/2020 3:26 PM

74. Unsolicited commercial e-mail, typically advertising transmitted in bulk, is called _____.
ANSWER: spam
POINTS: 1
REFERENCES: p. 11
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:01 PM
DATE MODIFIED: 12/27/2020 6:48 PM

75. The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information is called _____.
ANSWER: pharming
POINTS: 1
REFERENCES: p. 12
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Completion

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 7/20/2020 4:03 PM
DATE MODIFIED: 7/28/2020 3:24 PM

76. _____ are step-by-step instructions designed to assist employees in following policies, standards, and guidelines.
ANSWER: Procedures
POINTS: 1
REFERENCES: p. 13
H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Key Policy Components
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/20/2020 4:04 PM
DATE MODIFIED: 7/20/2020 4:05 PM

77. The _____ is the high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts.
ANSWER: enterprise information security policy (EISP)
EISP
enterprise information security policy
POINTS: 1
REFERENCES: p. 14
H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Key Policy Components
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 7/20/2020 3:40 PM
DATE MODIFIED: 8/1/2020 5:08 PM

78. _____ is the process of identifying and controlling the risks to an organization's information assets.
ANSWER: Risk management
POINTS: 1
REFERENCES: H1: OVERVIEW OF RISK MANAGEMENT
p. 19
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 5/19/2020 11:14 AM
DATE MODIFIED: 8/1/2020 5:01 PM

79. _____ is the selection of a strategy to address residual risk.
ANSWER: Risk treatment
POINTS: 1
REFERENCES: p. 21
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 5/19/2020 11:13 AM
DATE MODIFIED: 8/1/2020 5:02 PM

80. The selection of a strategy to address residual risk in an effort to bring it into alignment with the organization's risk appetite is known as _____.
ANSWER: risk treatment
POINTS: 1
REFERENCES: p. 21
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 4:06 PM
DATE MODIFIED: 7/20/2020 4:07 PM

81. Risk _____ is the assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.
ANSWER: tolerance
POINTS: 1
REFERENCES: p. 22
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Management and the RM Framework
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 4:08 PM
DATE MODIFIED: 7/20/2020 4:09 PM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

82. Within the context of risk management, any collection, set, or database of information or any asset that collects, stores, processes, or transmits information of value to the organization is known as a(n) _____.

ANSWER: information asset
POINTS: 1
REFERENCES: p. 24
H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 4:09 PM
DATE MODIFIED: 8/1/2020 5:02 PM

83. A threat _____ is an evaluation of the threats to information assets, including a determination of their likelihood of occurrence and potential impact of an attack.

ANSWER: assessment
POINTS: 1
REFERENCES: p. 28
H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 4:11 PM
DATE MODIFIED: 8/1/2020 5:03 PM

84. An understanding of the potential consequences of a successful attack on an information asset by a threat is called _____.

ANSWER: impact
POINTS: 1
REFERENCES: p. 30
H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 4:12 PM
DATE MODIFIED: 7/20/2020 4:13 PM

85. _____ is the state of having limited or imperfect knowledge of a situation, making it less likely that organizations can successfully anticipate future events or outcomes.

ANSWER: Uncertainty

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

POINTS: 1
REFERENCES: p. 33
H1: OVERVIEW OF RISK MANAGEMENT
H2: The RM Process
QUESTION TYPE: Completion
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 7/20/2020 4:14 PM
DATE MODIFIED: 8/1/2020 5:03 PM

Matching

Match each item with a statement below.

a. Threat agent b. Exploit
c. Hacker d. Virus
e. Trojan horse f. Risk management
g. Likelihood h. Residual risk
i. Standard

REFERENCES: H1: AN OVERVIEW OF INFORMATION SECURITY
H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H1: OVERVIEW OF RISK MANAGEMENT
QUESTION TYPE: Matching
HAS VARIABLES: False
LEARNING OBJECTIVES: 1.1 - Define and explain information security
1.2 - Describe the role of information security policy in the organization
1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 5/19/2020 11:42 AM
DATE MODIFIED: 12/27/2020 6:51 PM

86. A specific and identifiable instance of a general threat
ANSWER: a
POINTS: 1

87. A detailed statement of what must be done to comply with policy
ANSWER: i
POINTS: 1

88. A person who bypasses legitimate controls on an information system to gain access illegally
ANSWER: c
POINTS: 1

89. Something that looks like a desirable program or tool, but is in fact a malicious entity
ANSWER: e

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

POINTS: 1

90. The probability that a specific vulnerability within an organization will be successfully attacked
ANSWER: g
POINTS: 1

91. The risk that remains to an information asset even after an existing control has been applied
ANSWER: h
POINTS: 1

92. A means to target a specific vulnerability
ANSWER: b
POINTS: 1

93. The process used to identify and then control risks to an organization's information assets
ANSWER: f
POINTS: 1

94. A segment of code that performs malicious actions
ANSWER: d
POINTS: 1

Subjective Short Answer

95. What is a polymorphic threat?
ANSWER: A polymorphic threat is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and appearance to elude detection by antivirus software programs. This means that an e-mail generated by the virus may not match previous examples, making detection more of a challenge.
POINTS: 1
REFERENCES: p. 10
H1: AN OVERVIEW OF INFORMATION SECURITY
H2: The 12 Categories of Threats
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.1 - Define and explain information security
DATE CREATED: 12/27/2020 6:55 PM
DATE MODIFIED: 12/27/2020 7:06 PM

96. In order for policies to be effective and legally defensible, they must be properly:
ANSWER:
1. Developed using industry-accepted practices, and formally approved by management
2. Distributed using all appropriate methods
3. Read by all employees
4. Understood by all employees

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

5. Formally agreed to by act or affirmation
6. Uniformly applied and enforced

POINTS: 1
REFERENCES: H1: THE ROLE OF INFORMATION SECURITY POLICY IN DEVELOPING CONTINGENCY PLANS
H2: Guidelines for Effective Policy Development and Implementation
p. 15
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.2 - Describe the role of information security policy in the organization
DATE CREATED: 12/27/2020 6:57 PM
DATE MODIFIED: 12/27/2020 6:59 PM

97. Once the project team for information security development has created a ranked vulnerability worksheet, it must choose one of five approaches for controlling the risks that result from the vulnerabilities. List the five approaches.

ANSWER: The five approaches are:

- Defense
- Transference
- Mitigation
- Acceptance
- Termination

POINTS: 1
REFERENCES: p. 36
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 12/27/2020 6:59 PM
DATE MODIFIED: 12/27/2020 7:00 PM

98. Of the five major risk control strategies discussed in this module, which is the preferred strategy when it can be applied? Give some examples of techniques used in this approach.

ANSWER: The defense approach attempts to prevent the exploitation of a vulnerability. This is the preferred approach, and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards.

POINTS: 1
REFERENCES: p. 36
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank

Module 01 - An Overview of Information Security and Risk Management

LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 12/27/2020 7:00 PM
DATE MODIFIED: 12/27/2020 7:02 PM

99. Describe the transference approach to risk control and give three specific examples of risk transfer.
ANSWER: The risk transference approach attempts to shift the risk to other assets, other processes, or other organizations. This may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.
POINTS: 1
REFERENCES: p. 36
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 12/27/2020 7:02 PM
DATE MODIFIED: 12/27/2020 7:04 PM

100. Provide a list of the types of plans involved in the mitigation risk treatment strategy.
ANSWER:
1. The IR or incident response plan
2. The DR or disaster recovery plan
3. The BC or business continuity plan
4. The CM or crisis management plan

POINTS: 1
REFERENCES: p. 37
H1: OVERVIEW OF RISK MANAGEMENT
H2: Risk Treatment/Risk Control
QUESTION TYPE: Subjective Short Answer
HAS VARIABLES: False
STUDENT ENTRY MODE: Basic
LEARNING OBJECTIVES: 1.3 - Identify and explain the basic concepts and phases of risk management
DATE CREATED: 12/27/2020 7:04 PM
DATE MODIFIED: 12/27/2020 7:06 PM

Copyright Cengage Learning. Powered by Cognero.

Principles of Incident Response and Disaster Recovery 3rd edition Whitman Test Bank