Top of Form

Which technology would you implement to provide high availability for data storage?

Select one:

hot standby

software updates

RAID

N+1

#### Feedback

Refer to curriculum topic: 6.2.3  
System and data availability is a critical responsibility of a cybersecurity specialist. It is important to understand the technologies, process, and controls used to provide redundancy.

The correct answer is: RAID

### Question 2

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

An organization has recently adopted a five nines program for two critical database servers. What type of controls will this involve?

Select one:

limiting access to the data on these systems

stronger encryption systems

improving reliability and uptime of the servers

remote access to thousands of external users

#### Feedback

Refer to curriculum topic: 6.1.1  
System and data availability is a critical responsibility of a cybersecurity specialists. It is important to understand the technologies, process, and controls used to provide high availability.

The correct answer is: improving reliability and uptime of the servers

### Question 3

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which statement describes a characteristics of block ciphers?

Select one:

Block ciphers are faster than stream ciphers.

Block ciphers encrypt plaintext one bit at a time to form a block.

Block ciphers result in compressed output.

Block ciphers result in output data that is larger than the input data most of the time.

#### Feedback

Refer to curriculum topic: 4.1.2  
Encryption is an important technology used to protect confidentiality. It is important to understand the characteristics of the various encryption methodologies.

The correct answer is: Block ciphers result in output data that is larger than the input data most of the time.

### Question 4

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which protocol would be used to provide security for employees that access systems remotely from home?

Select one:

SCP

WPA

Telnet

SSH

#### Feedback

Refer to curriculum topic: 7.2.1  
Various application layer protocols are used to for communications between systems. A secure protocol provides a secure channel over an unsecured network.

The correct answer is: SSH

### Question 5

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which national resource was developed as a result of a U.S. Executive Order after a ten-month collaborative study involving over 3,000 security professionals?

Select one:

the National Vulnerability Database (NVD)

ISO OSI model

NIST Framework

ISO/IEC 27000

#### Feedback

Refer to curriculum topic: 8.3.1  
There are many tools that a cybersecurity specialist uses to evaluate the potential vulnerabilities of an organization.

The correct answer is: NIST Framework

### Question 6

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which statement best describes a motivation of hacktivists?

Select one:

They are trying to show off their hacking skills.

They are curious and learning hacking skills.

They are interested in discovering new exploits.

They are part of a protest group behind a political cause.

#### Feedback

Refer to curriculum topic: 1.2.1  
Each type of cybercriminal has a distinct motivation for his or her actions.

The correct answer is: They are part of a protest group behind a political cause.

### Question 7

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which wireless standard made AES and CCM mandatory?

Select one:

WEP

WPA

WPA2

WEP2

#### Feedback

Refer to curriculum topic: 7.1.2  
Wireless security depends on several industry standards and has progressed from WEP to WPA and finally WPA2.

The correct answer is: WPA2

### Question 8

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which threat is mitigated through user awareness training and tying security awareness to performance reviews?

Select one:

user-related threats

device-related threats

cloud-related threats

physical threats

#### Feedback

Refer to curriculum topic: 8.1.1  
Cybersecurity domains provide a framework for evaluating and implementing controls to protect the assets of an organization. Each domain has various countermeasures available to manage threats.

The correct answer is: user-related threats

### Question 9

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Your organization will be handling market trades. You will be required to verify the identify of each customer who is executing a transaction. Which technology should be implemented to authenticate and verify customer electronic transactions?

Select one:

symmetrical encryption

data hashing

digital certificates

asymmetrical encryption

#### Feedback

Refer to curriculum topic: 5.3.1  
Digital certificates protect the parties involved in secure communications.

The correct answer is: digital certificates

### Question 10

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Being able to maintain availability during disruptive events describes which of the principles of high availability?

Select one:

fault tolerance

uninterruptible services

single point of failure

system resiliency

#### Feedback

Refer to curriculum topic: 6.1.1  
High availability can be achieved by eliminating or reducing single points of failure, by implementing system resiliency, and by designing for fault tolerance.

The correct answer is: system resiliency

Bottom of Form

[Next page ►](https://lms.netacad.com/mod/quiz/review.php?attempt=3325888&cmid=5039611&page=1)

What type of application attack occurs when data goes beyond the memory areas allocated to the application?

Select one:

RAM Injection

buffer overflow

RAM spoofing

SQL injection

#### Feedback

Refer to curriculum topic: 3.3.3  
A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

The correct answer is: buffer overflow

### Question 12

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Your risk manager just distributed a chart that uses three colors to identify the level of threat to key assets in the information security systems. Red represents high level of risk, yellow represents average level of threat and green represents low level of threat. What type of risk analysis does this chart represent?

Select one:

exposure factor analysis

quantitative analysis

qualitative analysis

loss analysis

#### Feedback

Refer to curriculum topic: 6.2.1  
A quantitative or qualitative risk analysis is used to identify and prioritize threats to the organization.

The correct answer is: qualitative analysis

### Question 13

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What are the two most effective ways to defend against malware? (Choose two.)

Select one or more:

Implement RAID.

Update the operating system and other application software.

Implement network firewalls.

Implement strong passwords.

Install and update antivirus software.

Implement a VPN.

#### Feedback

Refer to curriculum topic: 3.1.1  
A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities.

The correct answers are: Update the operating system and other application software., Install and update antivirus software.

### Question 14

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

The X.509 standards defines which security technology?

Select one:

security tokens

strong passwords

biometrics

digital certificates

#### Feedback

Refer to curriculum topic: 5.3.2  
Digital certificates protect the parties involved in a secure communication

The correct answer is: digital certificates

### Question 15

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Mutual authentication can prevent which type of attack?

Select one:

wireless IP spoofing

man-in-the-middle

wireless poisoning

wireless sniffing

#### Feedback

Refer to curriculum topic: 7.1.2  
A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities.

The correct answer is: man-in-the-middle

### Question 16

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which technology can be used to ensure data confidentiality?

Select one:

identity management

encryption

hashing

RAID

#### Feedback

Refer to curriculum topic: 2.2.1  
A cybersecurity specialist must be aware of the technologies available which support the CIA triad.

The correct answer is: encryption

### Question 17

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

HVAC, water system, and fire systems fall under which of the cybersecurity domains?

Select one:

network

physical facilities

device

user

#### Feedback

Refer to curriculum topic: 8.1.6  
Cybersecurity domains provide a framework for evaluating and implementing controls to protect the assets of an organization.

The correct answer is: physical facilities

### Question 18

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

An organization has implemented antivirus software. What type of security control did the company implement?

Select one:

recovery control

detective control

compensative control

deterrent control

#### Feedback

Refer to curriculum topic: 4.2.7  
A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities.

The correct answer is: recovery control

### Question 19

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which data state is maintained in NAS and SAN services?

Select one:

data in-process

stored data

data in-transit

encrypted data

#### Feedback

Refer to curriculum topic: 2.3.1  
A cybersecurity specialist must be familiar with the types of technologies used to store, transmit, and process data.

The correct answer is: stored data

### Question 20

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

There are many environments that require five nines, but a five nines environment may be cost prohibitive. What is one example of where the five nines environment might be cost prohibitive?

Select one:

department stores at the local mall

the New York Stock Exchange

the front office of a major league sports team

the U.S. Department of Education

#### Feedback

Refer to curriculum topic: 6.1.1  
System and data availability is a critical responsibility of a cybersecurity specialist. It is important to understand the technologies, process, and controls used to protect provide high availability.

The correct answer is: the New York Stock Exchange

What type of attack has an organization experienced when an employee installs an unauthorized device on the network to view network traffic?

Select one:

sniffing

phishing

spoofing

spamming

#### Feedback

Refer to curriculum topic: 3.3.1  
A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

The correct answer is: sniffing

### Question 22

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

A VPN will be used within the organization to give remote users secure access to the corporate network. What does IPsec use to authenticate the origin of every packet to provide data integrity checking?

Select one:

salting

CRC

password

HMAC

#### Feedback

Refer to curriculum topic: 5.1.3  
HMAC is an algorithm used to authenticate. The sender and receiver have a secret key that is used along with the data to ensure the message origin as well as the authenticity of the data.

The correct answer is: HMAC

### Question 23

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which hashing algorithm is recommended for the protection of sensitive, unclassified information?

Select one:

SHA-256

MD5

3DES

AES-256

#### Feedback

Refer to curriculum topic: 5.1.1  
Data integrity is one of the three guiding security principles. A cybersecurity specialist should be familiar with the tools and technologies used to ensure data integrity.

The correct answer is: SHA-256

### Question 24

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which methods can be used to implement multifactor authentication?

Select one:

IDS and IPS

VPNs and VLANs

tokens and hashes

passwords and fingerprints

#### Feedback

Refer to curriculum topic: 2.2.1  
A cybersecurity specialist must be aware of the technologies available that support the CIA triad.

The correct answer is: passwords and fingerprints

### Question 25

Incorrect

Mark 0.00 out of 2.00

Flag question

#### Question text

What kind of integrity does a database have when all its rows have a unique identifier called a primary key?

Select one:

user-defined integrity

referential integrity

entity integrity

domain integrity

#### Feedback

Refer to curriculum topic: 5.4.1  
Data integrity is one of the three guiding security principles. A cybersecurity specialist should be familiar with the tools and technologies that are used to ensure data integrity.

The correct answer is: entity integrity

### Question 26

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

A specialist in the HR department is invited to promote the cybersecurity program in community schools. Which three topics would the specialist emphasize in the presentation to draw students to this field? (Choose three.)

Select one or more:

a field requiring a PhD degree

the CompTIA A+ certification provides an adequate knowledge base for the field

a job with routine, day-to-day tasks

high earning potential

service to the public

a career-field in high-demand

#### Feedback

Refer to curriculum topic: 1.2.2  
The increased demand for cybersecurity specialists offers several unique career opportunities.

The correct answers are: service to the public, high earning potential, a career-field in high-demand

### Question 27

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What are two incident response phases? (Choose two.)

Select one or more:

containment and recovery

risk analysis and high availability

detection and analysis

confidentiality and eradication

mitigation and acceptance

prevention and containment

#### Feedback

Refer to curriculum topic: 6.3.1  
When an incident occurs, the organization must know how to respond. An organization needs to develop an incident response plan that includes several phases.

The correct answers are: detection and analysis, containment and recovery

### Question 28

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Passwords, passphrases, and PINs are examples of which security term?

Select one:

identification

authentication

access

authorization

#### Feedback

Refer to curriculum topic: 4.2.4  
Authentication methods are used to strengthen access control systems. It is important to understand the available authentication methods.

The correct answer is: authentication

### Question 29

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which algorithm will Windows use by default when a user intends to encrypt files and folders in an NTFS volume?

Select one:

3DES

AES

DES

RSA

#### Feedback

Refer to curriculum topic: 4.1.4  
Encryption is an important technology used to protect confidentiality. It is important to understand the characteristics of the various encryption methodologies.

The correct answer is: AES

### Question 30

Incorrect

Mark 0.00 out of 2.00

Flag question

#### Question text

Which framework should be recommended for establishing a comprehensive information security management system in an organization?

Select one:

ISO/IEC 27000

CIA Triad

NIST/NICE framework

ISO OSI model

#### Feedback

Refer to curriculum topic: 2.5.1  
A cybersecurity specialist needs to be familiar with the different frameworks and models for managing information security.

The correct answer is: ISO/IEC 27000

Which technology can be implemented as part of an authentication system to verify the identification of employees?

Select one:

a smart card reader

a virtual fingerprint

a Mantrap

SHA-1 hash

#### Feedback

Refer to curriculum topic: 2.2.1  
A cybersecurity specialist must be aware of the technologies available that support the CIA triad.

The correct answer is: a smart card reader

### Question 32

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Users report that the database on the main server cannot be accessed. A database administrator verifies the issue and notices that the database file is now encrypted. The organization receives a threatening email demanding payment for the decryption of the database file. What type of attack has the organization experienced?

Select one:

ransomeware

Trojan horse

man-in-the-middle attack

DoS attack

#### Feedback

Refer to curriculum topic: 3.1.1  
A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

The correct answer is: ransomeware

### Question 33

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What is a feature of a cryptographic hash function?

Select one:

The hash input can be calculated given the output value.

The hash function is a one-way mathematical function.

Hashing requires a public and a private key.

The output has a variable length.

#### Feedback

Refer to curriculum topic: 5.1.1  
Data integrity is one of the three guiding security principles. A cybersecurity specialist should be familiar with the tools and technologies used to ensure data integrity.

The correct answer is: The hash function is a one-way mathematical function.

### Question 34

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

An organization wants to adopt a labeling system based on the value, sensitivity, and criticality of the information. What element of risk management is recommended?

Select one:

asset classification

asset availability

asset identification

asset standardization

#### Feedback

Refer to curriculum topic: 6.2.1  
One of the most important steps in risk management is asset classification.

The correct answer is: asset classification

### Question 35

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Smart cards and biometrics are considered to be what type of access control?

Select one:

logical

technological

physical

administrative

#### Feedback

Refer to curriculum topic: 4.2.1  
Access control prevents an unauthorized user from gaining access to sensitive data and networked systems. There are several technologies used to implement effective access control strategies.

The correct answer is: logical

### Question 36

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Alice and Bob use a pre-shared key to exchange a confidential message. If Bob wants to send a confidential message to Carol, what key should he use?

Select one:

the private key of Carol

a new pre-shared key

the same pre-shared key he used with Alice

the public key of Bob

#### Feedback

Refer to curriculum topic: 4.1.2  
Encryption is an important technology used to protect confidentiality. It is important to understand the characteristics of the various encryption methodologies.

The correct answer is: a new pre-shared key

### Question 37

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which utility uses the Internet Control Messaging Protocol (ICMP)?

Select one:

NTP

DNS

RIP

ping

#### Feedback

Refer to curriculum topic: 7.3.1  
ICMP is used by network devices to send error messages.

The correct answer is: ping

### Question 38

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What three best practices can help defend against social engineering attacks? (Choose three.)

Select one or more:

Do not provide password resets in a chat window.

Resist the urge to click on enticing web links.

Deploy well-designed firewall appliances.

Enable a policy that states that the IT department should supply information over the phone only to managers.

Add more security guards.

Educate employees regarding policies.

#### Feedback

Refer to curriculum topic: 3.2.2  
A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities.

The correct answers are: Educate employees regarding policies., Do not provide password resets in a chat window., Resist the urge to click on enticing web links.

### Question 39

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

The team is in the process of performing a risk analysis on the database services. The information collected includes the initial value of these assets, the threats to the assets and the impact of the threats. What type of risk analysis is the team performing by calculating the annual loss expectancy?

Select one:

quantitative analysis

protection analysis

qualitative analysis

loss analysis

#### Feedback

Refer to curriculum topic: 6.2.1  
A qualitative or quantitative risk analysis is used to identify and prioritize threats to the organization.

The correct answer is: quantitative analysis

### Question 40

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which method is used by steganography to hide text in an image file?

Select one:

least significant bit

most significant bit

data masking

data obfuscation

#### Feedback

Refer to curriculum topic: 4.3.2  
Encryption is an important technology used to protect confidentiality. It is important to understand the characteristics of the various encryption methodologies.

The correct answer is: least significant bit

You have been asked to implement a data integrity program to protect data files that need to be electronically downloaded by the sales staff. You have decided to use the strongest hashing algorithm available on your systems. Which hash algorithm would you select?

Select one:

SHA-1

SHA-256

MD5

AES

#### Feedback

Refer to curriculum topic: 5.1.1  
MD5 and SHA are the two most popular hashing algorithms. SHA-256 uses a 256-bit hash, whereas MD5 produces a 128-bit hash value.

The correct answer is: SHA-256

### Question 42

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which risk mitigation strategies include outsourcing services and purchasing insurance?

Select one:

avoidance

acceptance

reduction

transfer

#### Feedback

Refer to curriculum topic: 6.2.1  
Risk mitigation lessens the exposure of an organization to threats and vulnerabilities by transferring, accepting, avoiding, or taking an action to reduce risk.

The correct answer is: transfer

### Question 43

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which two protocols pose switching threats? (Choose two.)

Select one or more:

RIP

STP

ICMP

WPA2

IP

ARP

#### Feedback

Refer to curriculum topic: 7.3.1  
Network switches are the heart of the modern data communication network. The main threats to network switches are theft, hacking and remote access, and attacks against network protocols.

The correct answers are: ARP, STP

### Question 44

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which type of cybercriminal is the most likely to create malware to compromise an organization by stealing credit card information?

Select one:

black hat hackers

gray hat hackers

white hat hackers

script kiddies

#### Feedback

Refer to curriculum topic: 1.2.1  
Malware is a tool used by certain types of hackers to steal information.

The correct answer is: black hat hackers

### Question 45

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What is a nontechnical method that a cybercriminal would use to gather sensitive information from an organization?

Select one:

ransomeware

pharming

social engineering

man-in-the-middle

#### Feedback

Refer to curriculum topic: 3.2.1  
A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

The correct answer is: social engineering

### Question 46

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which three protocols can use Advanced Encryption Standard (AES)? (Choose three.)

Select one or more:

WEP

WPA2

802.11i

TKIP

802.11q

WPA

#### Feedback

Refer to curriculum topic: 7.3.1  
Various protocols can be used to provide secure communication systems. AES is the strongest encryption algorithm.

The correct answers are: 802.11i, WPA, WPA2

### Question 47

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which statement describes a distributed denial of service attack?"

Select one:

An attacker views network traffic to learn authentication credentials.

An attacker builds a botnet comprised of zombies.

An attacker sends an enormous quantity of data that a server cannot handle.

One computer accepts data packets based on the MAC address of another computer.

#### Feedback

Refer to curriculum topic: 3.3.1  
A cybersecurity specialist needs to be familiar with the characteristics of the different types of malware and attacks that threaten an organization.

The correct answer is: An attacker builds a botnet comprised of zombies.

### Question 48

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which technology could be used to prevent a cracker from launching a dictionary or brute-force attack off a hash?

Select one:

rainbow tables

MD5

AES

HMAC

#### Feedback

Refer to curriculum topic: 5.1.3  
HMACs use an additional secret key as input to the hash function. This adds another layer of security to the hash in order to defeat man-in-the-middle attacks and provide authentication of the data source.

The correct answer is: HMAC

### Question 49

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which technology can be used to protect VoIP against eavesdropping?

Select one:

encrypted voice messages

SSH

strong authentication

ARP

#### Feedback

Refer to curriculum topic: 7.3.2  
Many advanced technologies such as VoIP, streaming video, and electronic conferencing require advanced countermeasures.

The correct answer is: encrypted voice messages

### Question 50

Incorrect

Mark 0.00 out of 2.00

Flag question

#### Question text

An organization plans to implement security training to educate employees about security policies. What type of access control is the organization trying to implement?

Select one:

logical

technological

administrative

physical

#### Feedback

Refer to curriculum topic: 4.2.1  
Access control prevents an unauthorized user from gaining access to sensitive data and networked systems. There are several technologies used to implement effective access control strategies.

The correct answer is: administrative