# Final Quiz

| | | | |
|---|---|---|---|
| **Due** No due date | **Points** 100 | **Questions** 50 | **Time Limit** 60 Minutes |
| **Allowed Attempts** 2 | | | |

# Instructions

This quiz covers all of the content in **Cybersecurity Essentials 1.1.** It is designed to test the skills and knowledge presented in the course.

There are multiple task types that may be available in this quiz.

**NOTE:** Quizzes allow for partial credit scoring on all item types to foster learning. **Points on quizzes can also be deducted for answering incorrectly.**

Forms 32901 - 23908

> **Take the Quiz Again**

## Attempt History

| | Attempt | Time | Score |
|---|---|---|---|
| **LATEST** | **Attempt 1** | 28 minutes | 94 out of 100 |

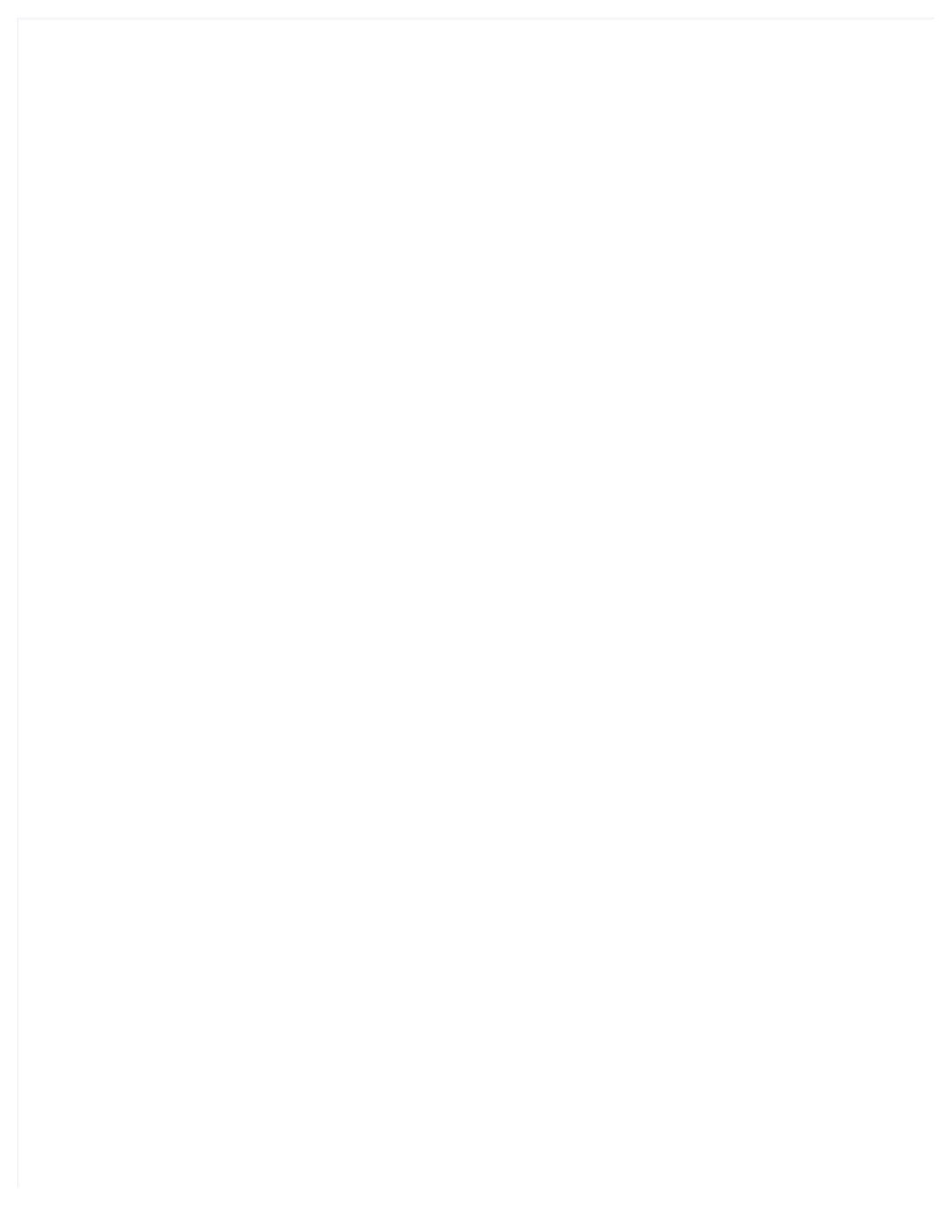Score for this attempt: **94** out of 100
Submitted Jul 20 at 3:25pm
This attempt took 28 minutes.

---

### Question 1                                                                 2 / 2 pts

Which statement best describes a motivation of hacktivists?

○ They are trying to show off their hacking skills.

○ They are interested in discovering new exploits.
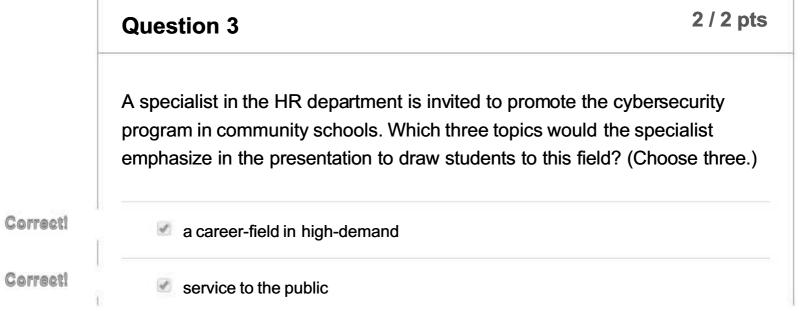
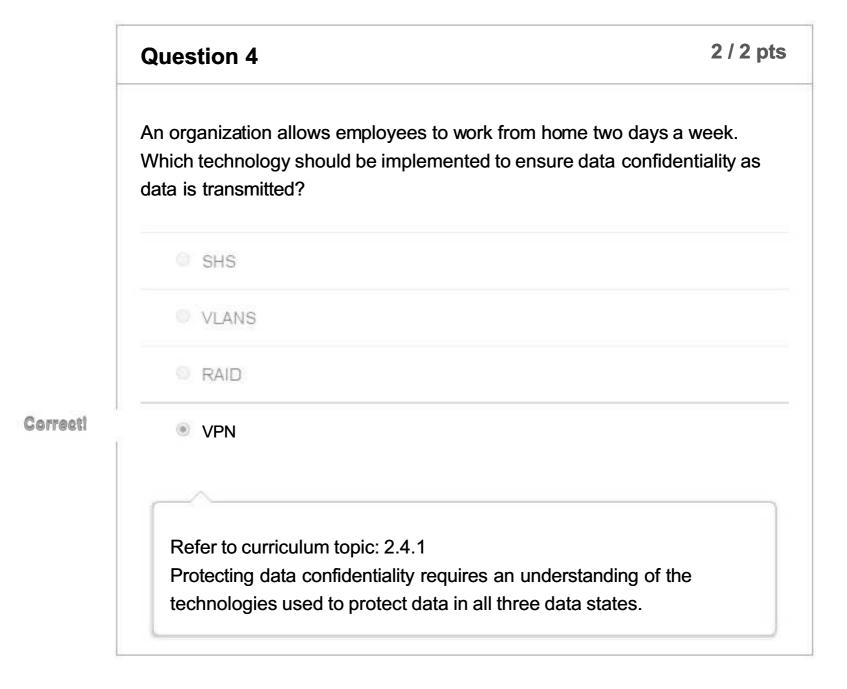○ They are curious and learning hacking skills.

**Correct!**  ● They are part of a protest group behind a political cause.

---

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

## Question 2                                           2 / 2 pts

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

- ○ white hat hackers

**Correct!**

- ● black hat hackers

- ○ gray hat hackers

- ○ script kiddies

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

## Question 3                                           2 / 2 pts

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.)

**Correct!**

- ☑ a career-field in high-demand

**Correct!**

- ☑ service to the public

**Correct!**

☑ high earning potential

☐ a job with routine, day-to-day tasks

☐ a field requiring a PhD degree

☐ the CompTIA A+ certification provides an adequate knowledge base for the field
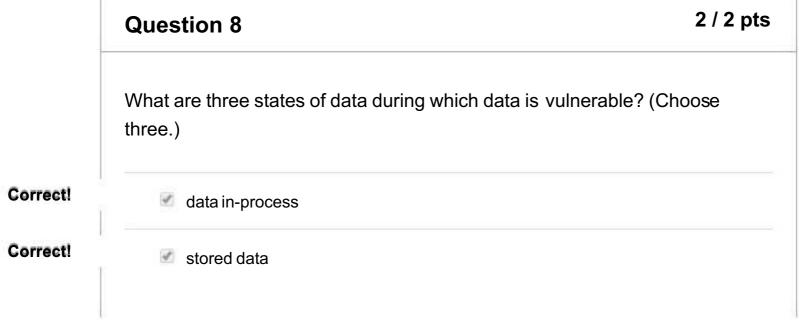
> Refer to curriculum topic: 1.2.2
> The increased demand for cybersecurity specialists offers several unique career opportunities.

## Question 4

2 / 2 pts

An organization allows employees to work from home two days a week. Which technology should be implemented to ensure data confidentiality as data is transmitted?

○ SHS

○ VLANS

○ RAID

**Correct!**

◉ VPN

> Refer to curriculum topic: 2.4.1
> Protecting data confidentiality requires an understanding of the technologies used to protect data in all three data states.

## Question 5

**2 / 2 pts**

Which type of networks poses increasing challenges to cybersecurity specialists due to the growth of BYOD on campus?

**Correct!**

- ◉ wireless networks

- ○ wired networks

- ○ sneaker net

- ○ virtual networks

Refer to curriculum topic: 2.3.2

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

## Question 6

**2 / 2 pts**

A cybersecurity specialist is working with the IT staff to establish an effective information security plan. Which combination of security principles forms the foundation of a security plan?

**Correct!**

- ◉ confidentiality, integrity, and availability

- ○ technologies, policies, and awareness

- ○ secrecy, identify, and nonrepudiation

- ○ encryption, authentication, and identification

Refer to curriculum topic: 2.1.1
The CIA Triad is the foundation upon which all information management systems are developed.

## Question 7

**2 / 2 pts**

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

**Correct!**

- ⦿ ISO/IEC 27000

- ○ ISO OSI model

- ○ NIST/NICE framework

- ○ CIA Triad

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

## Question 8

**2 / 2 pts**

What are three states of data during which data is vulnerable? (Choose three.)

**Correct!**

- ☑ data in-process

**Correct!**

- ☑ stored data

**Correct!**

☑ data in-transit

☐ data encrypted

☐ purged data

☐ data decrypted

Refer to curriculum topic: 2.3.1
A cybersecurity specialist must be aware of each of the three states of data to effectively protect data and information. Purged data was stored data. Encrypted and decrypted data can be in any of the three states.

---

## Question 9                                                    2 / 2 pts

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?

○ man-in-the-middle attack

**Correct!**    ● ransomeware

○ Trojan horse

○ DoS attack

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.

## Question 10                                                      2 / 2 pts

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

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

☐ Add more security guards.

**Correct!**    ☑ Resist the urge to click on enticing web links.

☐ Deploy well-designed firewall appliances.

**Correct!**    ☑ Educate employees regarding policies.

**Correct!**    ☑ Do not provide password resets in a chat window.

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.

## Question 11                                                      2 / 2 pts

Which statement describes a distributed denial of service attack?"

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

**Correct!**

◉ An attacker builds a botnet comprised of zombies.

○ An attacker views network traffic to learn authentication credentials.

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

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.

---

## Question 12                                    2 / 2 pts

A cyber criminal sends a series of maliciously formatted packets to the database server. The server cannot parse the packets and the event causes the server crash. What is the type of attack the cyber criminal launches?

**Correct!**

◉ DoS

○ man-in-the-middle

○ packet Injection

○ SQL injection

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.

## Question 13                                           0 / 2 pts

An executive manager went to an important meeting. The secretary in the office receives a call from a person claiming that the executive manager is about to give an important presentation but the presentation files are corrupted. The caller sternly recommends that the secretary email the presentation right away to a personal email address. The caller also states that the executive is holding the secretary responsible for the success of this presentation. Which type of social engineering tactic would describe this scenario?

**ou Answered**

⦿  urgency

**orrect Answer**

◯  intimidation

◯  familiarity

◯  trusted partners

Refer to curriculum topic: 3.2.1
Social engineering uses several different tactics to gain information from victims.

## Question 14                                           2 / 2 pts

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

☐ Implement network firewalls.

**Correct!**
☑ Install and update antivirus software.

☐ Implement RAID.

**Correct!**
☑ Update the operating system and other application software.

☐ Implement strong passwords.

☐ Implement a VPN.

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.

## Question 15                                2 / 2 pts

The employees in a company receive an email stating that the account password will expire immediately and requires a password reset within 5 minutes. Which statement would classify this email?

○ It is a piggy-back attack.

○ It is an impersonation attack.

○ It is a DDoS attack.

**Correct!**
◉ It is a hoax.

Refer to curriculum topic: 3.2.2
Social engineering uses several different tactics to gain information from victims.

## Question 16

**2 / 2 pts**

In which situation would a detective control be warranted?

**Correct!**

- ⦿ when the organization needs to look for prohibited activity

- ○ after the organization has experienced a breach in order to restore everything back to a normal state

- ○ when the organization cannot use a guard dog, so it is necessary to consider an alternative

- ○ when the organization needs to repair damage

Refer to curriculum topic: 4.2.7
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.

## Question 17

**2 / 2 pts**

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

**Correct!**

○ ● recovery control

○ deterrent control

○ detective control

○ compensative control

> 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.

## Question 18

**2 / 2 pts**

Alice and Bob are using public key encryption to exchange a message. Which key should Alice use to encrypt a message to Bob?

○ the private key of Alice

**Correct!**

○ ● the public key of Bob

○ the private key of Bob

○ the public key of Alice

> Refer to curriculum topic: 4.1.3
> Encryption is an important technology used to protect confidentiality. It is important to understand the characteristics of the various encryption methodologies.

## Question 19                                                            2 / 2 pts

Which statement describes a characteristics of block ciphers?

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

**Correct!**

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

○ Block ciphers result in compressed output.

○ Block ciphers are faster than stream ciphers.

> 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.

## Question 20                                                            2 / 2 pts

The IT department is tasked to implement a system that controls what a user can and cannot do on the corporate network. Which process should be implemented to meet the requirement?

○ user login auditing

**Correct!**

◉ a set of attributes that describes user access rights

○ observations to be provided to all employees

○ a biometric fingerprint reader

Refer to curriculum topic: 4.2.5
Access control prevents unauthorized user from gaining access to sensitive data and networked systems. There are several technologies used to implement effective access control strategies.

## Question 21

**2 / 2 pts**

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?

○ the same pre-shared key he used with Alice

○ the private key of Carol

**Correct!**

◉ a new pre-shared key

○ the public key of Bob

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.

## Question 22

**2 / 2 pts**

Which access control strategy allows an object owner to determine whether to allow access to the object?

○ RBAC

**Correct!**

     ◉   DAC

     ○   MAC

     ○   ACL

Refer to curriculum topic: 4.2.2

Access control prevents unauthorized user from gaining access to sensitive data and networked systems. There are several technologies used to implement effective access control strategies.

### Question 23

**2 / 2 pts**

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

     ○   data obfuscation

     ○   data masking

**Correct!**      ◉   least significant bit

     ○   most significant bit

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.

### Question 24

**2 / 2 pts**

The X.509 standards defines which security technology?

**Correct!**

- ● digital certificates

- ○ biometrics

- ○ strong passwords

- ○ security tokens

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

## Question 25

**2 / 2 pts**

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

- ○ MD5

- ○ AES-256

- ○ 3DES

**Correct!**

- ● SHA-256

> 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.

## Question 26

**2 / 2 pts**

Technicians are testing the security of an authentication system that uses passwords. When a technician examines the password tables, the technician discovers the passwords are stored as hash values. However, after comparing a simple password hash, the technician then discovers that the values are different from those on other systems. What are two causes of this situation? (Choose two.)

☐ Both systems scramble the passwords before hashing.

**Correct!**

☑ The systems use different hashing algorithms.

**Correct!**

☑ One system uses hashing and the other uses hashing and salting.
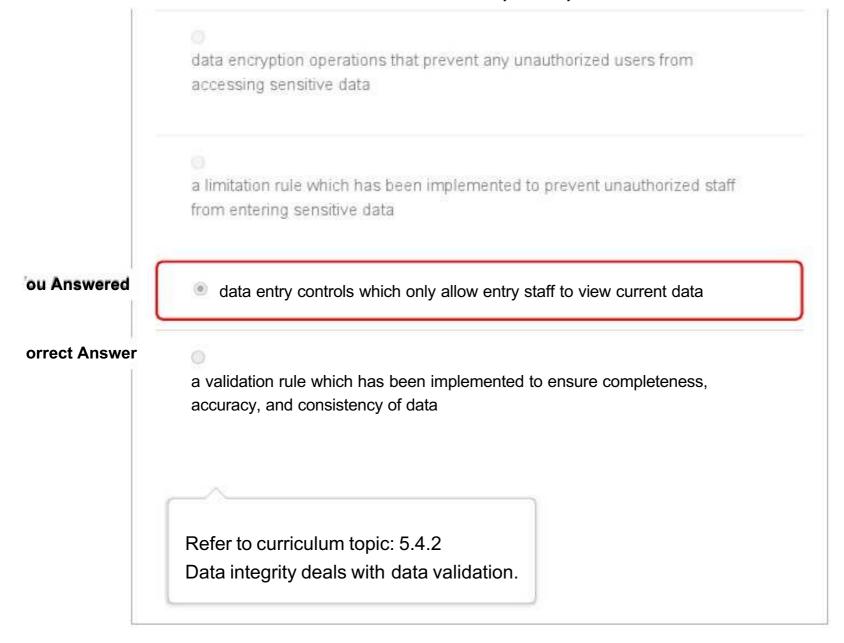
☐ Both systems use MD5.

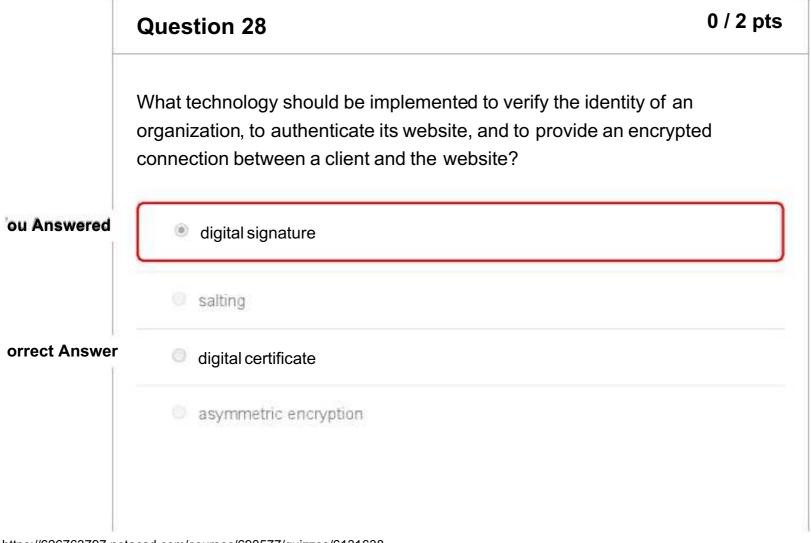☐ One system uses symmetrical hashing and the other uses asymmetrical hashing.

Refer to curriculum topic: 5.1.2
Hashing can be used in many different situations to ensure data integrity.

## Question 27

**0 / 2 pts**

You have been asked to work with the data collection and entry staff in your organization in order to improve data integrity during initial data entry and data modification operations. Several staff members ask you to explain why the new data entry screens limit the types and size of data able to be entered in specific fields. What is an example of a new data integrity control?

data encryption operations that prevent any unauthorized users from accessing sensitive data

a limitation rule which has been implemented to prevent unauthorized staff from entering sensitive data

**ou Answered**

◉ data entry controls which only allow entry staff to view current data

**orrect Answer**

a validation rule which has been implemented to ensure completeness, accuracy, and consistency of data

Refer to curriculum topic: 5.4.2
Data integrity deals with data validation.

## Question 28     0 / 2 pts

What technology should be implemented to verify the identity of an organization, to authenticate its website, and to provide an encrypted connection between a client and the website?

**ou Answered**

◉ digital signature

salting

**orrect Answer**

digital certificate

asymmetric encryption

Refer to curriculum topic: 5.2.2
Encryption is an important technology used to protect confidentiality. It is important to understand the characteristics of the various encryption methodologies.

## Question 29                                                    2 / 2 pts

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?

○ data hashing

○ asymmetrical encryption

○ symmetrical encryption

**Correct!**          ● digital certificates

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

## Question 30                                                    2 / 2 pts

Alice and Bob are using a digital signature to sign a document. What key should Alice use to sign the document so that Bob can make sure that the document came from Alice?

○ public key from Bob

**Correct!** ◉ private key from Alice

○ username and password from Alice

○ private key from Bob

Refer to curriculum topic: 5.2.2
Alice and Bob are used to explain asymmetric cryptography used in digital signatures. Alice uses a private key to encrypt the message digest. The message, encrypted message digest, and the public key are used to create the signed document and prepare it for transmission.

## Question 31                                    2 / 2 pts

An organization has determined that an employee has been cracking passwords on administrative accounts in order to access very sensitive payroll information. Which tools would you look for on the system of the employee? (Choose three)

**Correct!** ☑ rainbow tables

**Correct!** ☑ lookup tables

☐ algorithm tables

☐ password digest

☐ rouge access points

**Correct!** ☑ reverse lookup tables

Refer to curriculum topic: 5.1.2
Tables that contain possible password combinations are used to crack passwords.

## Question 32

**2 / 2 pts**

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?

**Correct!**

- ◉ asset classification

- ○ asset identification

- ○ asset availability

- ○ asset standardization

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

## Question 33

**2 / 2 pts**

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

- ○ stronger encryption systems

**Correct!**

- ◉ improving reliability and uptime of the servers

○ remote access to thousands of external users

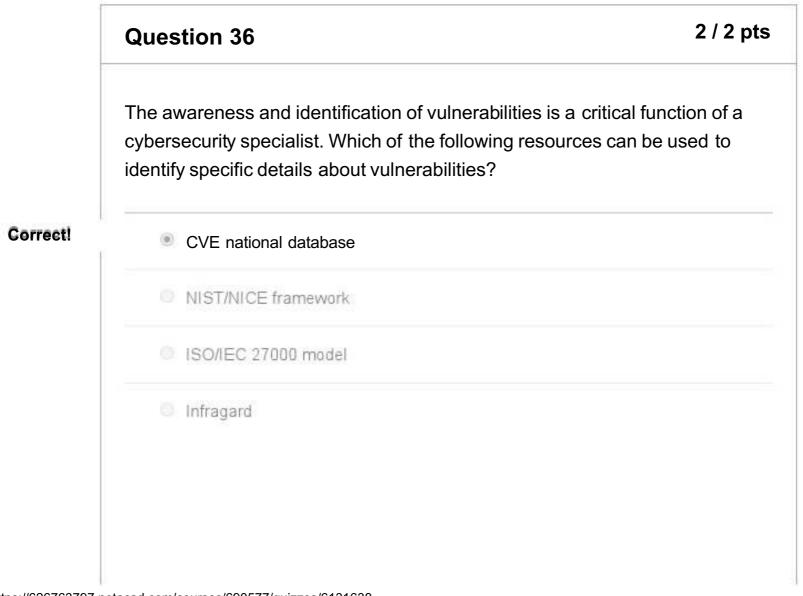○ limiting access to the data on these systems

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.

## Question 34                                      2 / 2 pts

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

○ single point of failure

**Correct!**          ● system resiliency

○ fault tolerance

○ uninterruptible services

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.

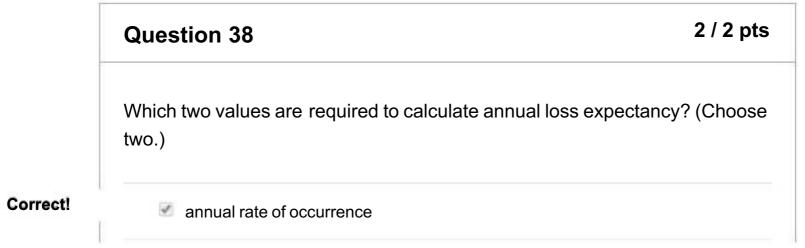## Question 35                                      2 / 2 pts

Which risk mitigation strategies include outsourcing services and purchasing insurance?

**Correct!**

○ avoidance

◉ transfer

○ reduction

○ acceptance

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.

---

### Question 36                                                2 / 2 pts

The awareness and identification of vulnerabilities is a critical function of a cybersecurity specialist. Which of the following resources can be used to identify specific details about vulnerabilities?

**Correct!**

◉ CVE national database

○ NIST/NICE framework

○ ISO/IEC 27000 model

○ Infragard

Refer to curriculum topic: 6.2.1
A cybersecurity specialist needs to be familiar with the resources such as the CVE database, Infragard, and the NIST/NISE framework. All can be used to help plan and implement effective an information security management system.

## Question 37

**2 / 2 pts**

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

○ N+1

○ software updates

**Correct!**

◉ RAID

○ hot standby

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.

## Question 38

**2 / 2 pts**

Which two values are required to calculate annual loss expectancy? (Choose two.)

**Correct!**

☑ annual rate of occurrence

☐ asset value

☐ frequency factor

☐ exposure factor

**Correct!**          ☑ single loss expectancy

☐ quantitative loss value

Refer to curriculum topic: 6.2.1
Single loss expectancy, annualized rate of occurrence, and
annualized loss expectancy are used in a quantitative risk analysis

---

## Question 39                                    2 / 2 pts

What is it called when an organization only installs applications that meet its
guidelines, and administrators increase security by eliminating all other
applications?

○ asset availability

○ asset identification

○ asset classification

**Correct!**          ◉ asset standardization

Refer to curriculum topic: 6.2.1
An organization needs to know what hardware and software are present as a prerequisite to knowing what the configuration parameters need to be. Asset management includes a complete inventory of hardware and software. Asset standards identify specific hardware and software products that the organization uses and supports. When a failure occurs, prompt action helps to maintain both access and security.

## Question 40

2 / 2 pts

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?

- ○ department stores at the local mall

- ○ the front office of a major league sports team

- ○ the U.S. Department of Education

**Correct!**

- ⦿ the New York Stock Exchange

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.

## Question 41

2 / 2 pts

Which technology can be used to protect VoIP against eavesdropping?

○ ARP

**Correct!**          ◉ encrypted voice messages

○ strong authentication

○ SSH

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

---

## Question 42                                              2 / 2 pts

Mutual authentication can prevent which type of attack?

○ wireless poisoning

○ wireless IP spoofing

○ wireless sniffing

**Correct!**          ◉ man-in-the-middle

> 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.
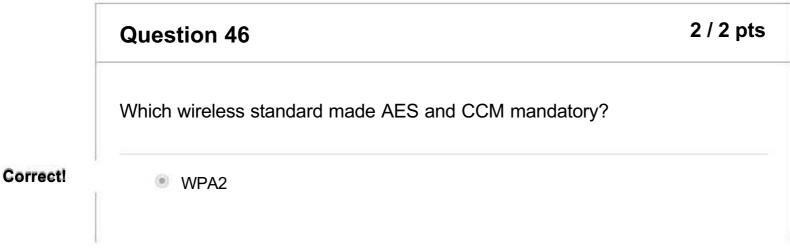
---

## Question 43                                              2 / 2 pts

Which of the following products or technologies would you use to establish a baseline for an operating system?

**Correct!**

○ SANS Baselining System (SBS)

◉ Microsoft Security Baseline Analyzer

○ MS Baseliner

○ CVE Baseline Analyzer

> Refer to curriculum topic: 7.1.1
> There are many tools that a cybersecurity specialist uses to evaluate the potential vulnerabilities of an organization.

## Question 44                                                   2 / 2 pts

What Windows utility should be used to configure password rules and account lockout policies on a system that is not part of a domain?

○ Active Directory Security tool

○ Computer Management

**Correct!**

◉ Local Security Policy tool
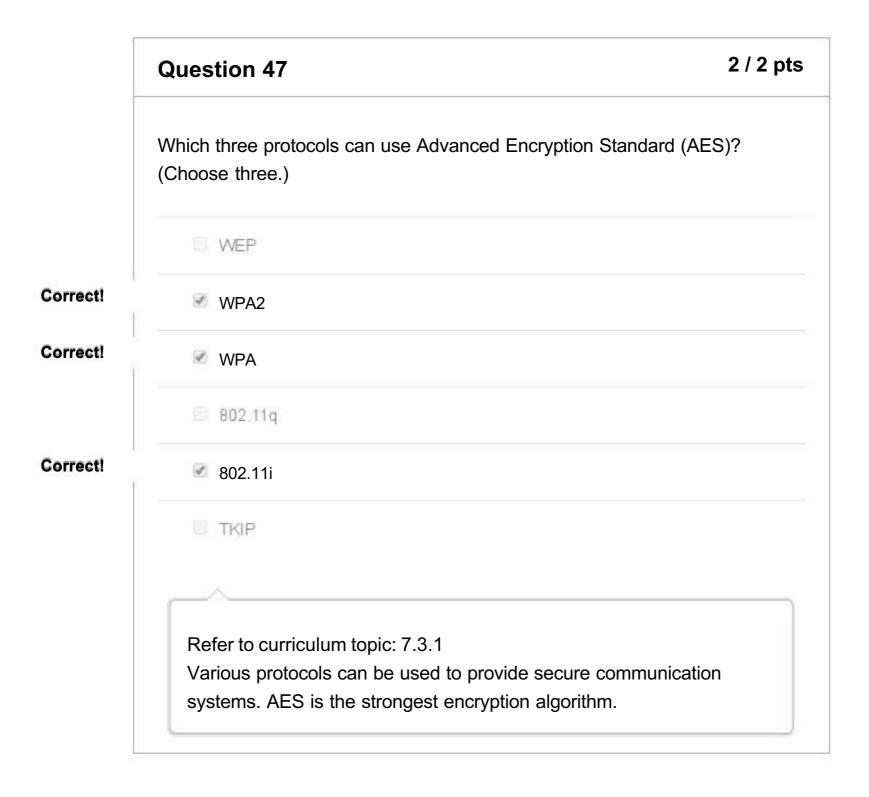
○ Event Viewer security log

Refer to curriculum topic: 7.2.2
A cybersecurity specialist must be aware of the technologies and
measures that are used as countermeasures to protect the
organization from threats and vulnerabilities. Local Security Policy,
Event Viewer, and Computer Management are Windows utilities that
are all used in the security equation.

## Question 45

2 / 2 pts

What describes the protection provided by a fence that is 1 meter in height?

Correct!

⦿ It deters casual trespassers only.

○ It prevents casual trespassers because of its height.

○ The fence deters determined intruders.

○ It offers limited delay to a determined intruder.

Refer to curriculum topic: 7.4.1
Security standards have been developed to assist organizations in
implementing the proper controls to mitigate potential threats. The
height of a fence determines the level of protection from intruders

## Question 46

2 / 2 pts

Which wireless standard made AES and CCM mandatory?

Correct!

⦿ WPA2

○ WEP

○ WEP2

○ WPA

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

## Question 47                                          2 / 2 pts

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

☐ WEP

**Correct!**  ☑ WPA2

**Correct!**  ☑ WPA

☐ 802.11q

**Correct!**  ☑ 802.11i

☐ TKIP

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

## Question 48                                                    2 / 2 pts

Which website offers guidance on putting together a checklist to provide
guidance on configuring and hardening operating systems?

○ Internet Storm Center

○ The Advanced Cyber Security Center

**Correct!**

  ● The National Vulnerability Database website

○ CERT

Refer to curriculum topic: 8.2.3
There are several cybersecurity information websites that a
cybersecurity specialist uses to evaluate the potential vulnerabilities of
an organization. Some of these websites are the National Vulnerability
Database, CERT, the Internet Storm Center, and the Advanced Cyber
Security Center.

## Question 49                                                    2 / 2 pts

Which law was enacted to prevent corporate accounting-related crimes?

○ The Federal Information Security Management Act

○ Gramm-Leach-Bliley Act

○ Import/Export Encryption Act

**Correct!**

  ● Sarbanes-Oxley Act