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

Attempt History

	Attempt	Time	Score
KEPT	Attempt 2	25 minutes	94 out of 100
LATEST	Attempt 2	25 minutes	94 out of 100
	Attempt 1	20 minutes	60.67 out of 100

Score for this attempt: **94** out of 100
Submitted Feb 1 at 4:20pm
This attempt took 25 minutes.

Question 1

2 / 2 pts

Technologies like GIS and IoE contribute to the growth of large data stores. What are two reasons that these technologies increase the need for cybersecurity specialists? (Choose two.)

Correct! ☑ They collect sensitive information.

Correct! ☑ They contain personal information.

☐ They make systems more complicated.

☐ They require 24-hour monitoring.

- [ ] They increase processing requirements.
- [ ] They require more equipment.

Refer to curriculum topic: 1.1.1
The types of information collected by these technologies have increased the need for data protection.

Question 2

2 / 2 pts

Which two groups of people are considered internal attackers? (Choose two.)

- [ ] black hat hackers
- [ ] hacktivists
- [x] trusted partners

Correct!

- [x] ex-employees

Correct!

- [ ] amateurs

Refer to curriculum topic: 1.4.1
Threats are classified as being from an internal source or external source. A cybersecurity specialist needs to be aware of the source of various threats.

Question 3

2 / 2 pts

Which statement best describes a motivation of hacktivists?

- [ ] They are curious and learning hacking skills.

Correct!

- They are part of a protest group behind a political cause.
- They are interested in discovering new exploits.
- They are trying to show off their hacking skills.

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

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?

- RAID

Correct!

- VPN
- SHS
- VLANS

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 data state is maintained in NAS and SAN services?

data in-transit

Correct!

stored data

encrypted data

data in-process

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.

Question 6

2 / 2 pts

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

Correct!

a smart card reader

a virtual fingerprint

a Mantrap

SHA-1 hash

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

Question 7

2 / 2 pts

Which methods can be used to implement multifactor authentication?

Correct!

- passwords and fingerprints
- VPNs and VLANs
- IDS and IPS
- tokens and hashes

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

Question 8

2 / 2 pts

Which technology can be used to ensure data confidentiality?

Correct!

- encryption
- identity management
- hashing
- RAID

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

Question 9

2 / 2 pts

What type of attack will make illegitimate websites higher in a web search result list?

browser hijacker

Correct!

SEO poisoning

spam

DNS poisoning

Refer to curriculum topic: 3.1.2
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

A penetration testing service hired by the company has reported that a backdoor was identified on the network. What action should the organization take to find out if systems have been compromised?

Correct!

Look for unauthorized accounts.

Look for usernames that do not have passwords.

Look for policy changes in Event Viewer.

Scan the systems for viruses.

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 11

2 / 2 pts

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

Correct!

- (•) social engineering
- ( ) ransomeware
- ( ) man-in-the-middle
- ( ) pharming

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.

Question 12

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 an impersonation attack.

Correct!

- (•) It is a hoax.
- ( ) It is a piggy-back attack.
- ( ) It is a DDoS attack.

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

Question 13

2 / 2 pts

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

- [ ] Implement strong passwords.
- [x] Update the operating system and other application software.

Correct!

- [ ] Implement network firewalls.
- [ ] Implement RAID.
- [x] Install and update antivirus software.

Correct!

- [ ] 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 14

2 / 2 pts

What is an impersonation attack that takes advantage of a trusted relationship between two systems?

- ( ) man-in-the-middle
- ( ) sniffing
- ( ) spamming
- (•) spoofing

Correct!

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 15

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?

- Trojan horse
- DoS attack
- man-in-the-middle attack
- ransomeware

Correct!

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 16

2 / 2 pts

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

- most significant bit

data obfuscation

data masking

Correct!

least 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 17

2 / 2 pts

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

Correct!

authentication

identification

access

authorization

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.

Question 18

2 / 2 pts

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

ACL

Correct! DAC

RBAC

MAC

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 19

2 / 2 pts

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

compensative control

detective control

deterrent control

Correct! recovery 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 20

0 / 2 pts

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

- administrative
- technological

orrect Answer

- logical

'ou Answered

- physical

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.

Question 21

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?

Correct!

- the public key of Bob
- the public key of Alice
- the private key of Bob
- the private 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 22

2 / 2 pts

What happens as the key length increases in an encryption application?

- Keyspace decreases proportionally.
- Correct! Keyspace increases exponentially.
- Keyspace decreases exponentially.
- Keyspace increases proportionally.

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.

Question 23

2 / 2 pts

In which situation would a detective control be warranted?

- 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
- Correct! when the organization needs to look for prohibited activity

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 24

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?

- private key from Bob
- Correct! private key from Alice
- public key from Bob
- username and password from Alice

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 25

2 / 2 pts

What technology should you implement to ensure that an individual cannot later claim that he or she did not sign a given document?

- Correct! digital signature

asymmetric encryption

HMAC

digital certificate

Refer to curriculum topic: 5.2.1
A digital signature is used to establish authenticity, integrity, and nonrepudiation.

Question 26

2 / 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 entry controls which only allow entry staff to view current data

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

Correct!

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 27

2 / 2 pts

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?

- salting
- CRC
- HMAC

Correct!

- password

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.

Question 28

2 / 2 pts

The X.509 standards defines which security technology?

- security tokens
- digital certificates

Correct!

- strong passwords

biometrics

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

Question 29

2 / 2 pts

Which hashing technology requires keys to be exchanged?

MD5

Correct!

HMAC

AES

salting

Refer to curriculum topic: 5.1.3
The difference between HMAC and hashing is the use of keys.

Question 30

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!

reverse lookup tables

password digest

Correct!

- [x] lookup tables

Correct!

- [x] rainbow tables
- [ ] rouge access points
- [ ] algorithm tables

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

Question 31

2 / 2 pts

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?

Correct!

- (•) SHA-256
- ( ) MD5
- ( ) AES
- ( ) SHA-1

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.

Question 32

2 / 2 pts

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

Correct!

- [x] single loss expectancy
- [ ] asset value
- [ ] quantitative loss value

Correct!

- [x] annual rate of occurrence
- [ ] frequency factor
- [ ] exposure factor

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 33

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?

- ( ) NIST/NICE framework

Correct!

- (•) CVE national database
- ( ) Infragard
- ( ) ISO/IEC 27000 model

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 34

2 / 2 pts

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

- uninterruptible services
- system resiliency

Correct!

- single point of failure
- fault tolerance

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

- hot standby
- software updates

N+1

Correct!

RAID

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 36

2 / 2 pts

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?

loss analysis

exposure factor analysis

quantitative analysis

Correct!

qualitative analysis

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

Question 37

2 / 2 pts

What approach to availability provides the most comprehensive protection

because multiple defenses coordinate together to prevent attacks?

- obscurity
- Correct! layering
- diversity
- limiting

Refer to curriculum topic: 6.2.2
Defense in depth utilizes multiple layers of security controls.

Question 38

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?

- the front office of a major league sports team
- Correct! the New York Stock Exchange
- department stores at the local mall
- the U.S. Department of Education

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 39

2 / 2 pts

What approach to availability involves using file permissions?

- simplicity
- limiting

Correct!

- obscurity
- layering

Refer to curriculum topic: 6.2.2
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 40

0 / 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 classification
- asset identification
- asset availability

ou Answered

- asset standardization

orrect Answer

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 41

2 / 2 pts

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

Correct!

- (•) ping
- ( ) RIP
- ( ) NTP
- ( ) DNS

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

Question 42

2 / 2 pts

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

- ( ) CVE Baseline Analyzer

Correct!

- (•) Microsoft Security Baseline Analyzer

SANS Baselining System (SBS)

MS Baseliner

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 43

2 / 2 pts

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

RIP

WPA2

Correct! STP

ICMP

IP

Correct! ARP

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.

Question 44

2 / 2 pts

Mutual authentication can prevent which type of attack?

Correct!

- man-in-the-middle
- wireless poisoning
- wireless IP spoofing
- wireless sniffing

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 45

2 / 2 pts

Which wireless standard made AES and CCM mandatory?

- WPA
- WEP2
- WEP

Correct!

- WPA2

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 46

2 / 2 pts

Which protocol would be used to provide security for employees that access

systems remotely from home?

- Telnet
- WPA
- SSH

Correct!

- SCP

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.

Question 47

0 / 2 pts

In a comparison of biometric systems, what is the crossover error rate?

- rate of acceptability and rate of false negatives

orrect Answer

- rate of false negatives and rate of false positives
- rate of rejection and rate of false negatives

'ou Answered

- rate of false positives and rate of acceptability

Refer to curriculum topic: 7.4.1
In comparing biometric systems, there are several important factors to consider including accuracy, speed or throughput rate, and acceptability to users.

Question 48

2 / 2 pts

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

- cloud-related threats
- physical threats
- device-related threats
- user-related threats

Correct!

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.

Question 49

2 / 2 pts

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

- CERT
- Internet Storm Center
- The Advanced Cyber Security Center
- The National Vulnerability Database website

Correct!

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 50

2 / 2 pts

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

Correct!

- (•) Sarbanes-Oxley Act
- ( ) Import/Export Encryption Act
- ( ) The Federal Information Security Management Act
- ( ) Gramm-Leach-Bliley Act

Refer to curriculum topic: 8.2.2
New laws and regulations have come about to protect organizations, citizens, and nations from cybersecurity attacks.

Quiz Score: **94** out of 100