What approach to availability provides the most comprehensive protection because multiple defenses coordinate together to prevent attacks?

Select one:

limiting

diversity

obscurity

layering

#### Feedback

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

The correct answer is: layering

### Question 2

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What is the most difficult part of designing a cryptosystem?

Select one:

reverse engineering

key length

key management

encryption algorithm

#### Feedback

Refer to curriculum topic: 4.1.1  
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: key management

### Question 3

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

sneaker net

virtual networks

wireless networks

wired networks

#### Feedback

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.

The correct answer is: wireless networks

### Question 4

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

man-in-the-middle

spamming

sniffing

spoofing

#### 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: spoofing

### Question 5

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one or more:

single loss expectancy

frequency factor

quantitative loss value

annual rate of occurrence

exposure factor

asset value

#### Feedback

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

The correct answers are: single loss expectancy, annual rate of occurrence

### Question 6

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

VLANS

RAID

VPN

SHS

#### Feedback

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.

The correct answer is: VPN

### Question 7

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

private key from Bob

public key from Bob

private key from Alice

username and password from Alice

#### Feedback

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.

The correct answer is: private key from Alice

### Question 8

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:

Telnet

SCP

SSH

WPA

#### 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 9

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one or more:

ex-employees

hacktivists

amateurs

black hat hackers

trusted partners

#### Feedback

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.

The correct answers are: trusted partners, ex-employees

### Question 10

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

You have been asked to describe data validation to the data entry clerks in accounts receivable. Which of the following are good examples of strings, integers, and decimals?

Select one:

female, 9866, $125.50

male, $25.25, veteran

yes/no 345-60-8745, TRF562

800-900-4560, 4040-2020-8978-0090, 01/21/2013

#### Feedback

Refer to curriculum topic: 5.4.2  
A string is a group of letters, numbers and special characters. An integer is whole number.  A decimal is a  number that is not a fraction.

The correct answer is: female, 9866, $125.50

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?

Select one:

It is a DDoS attack.

It is an impersonation attack.

It is a hoax.

It is a piggy-back attack.

#### Feedback

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

The correct answer is: It is a hoax.

### Question 12

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

A security specialist is asked for advice on a security measure to prevent unauthorized hosts from accessing the home network of employees. Which measure would be most effective?

Select one:

Implement a VLAN.

Implement RAID.

Implement intrusion detection systems.

Implement a firewall.

#### Feedback

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.

The correct answer is: Implement a firewall.

### Question 13

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

Internet Storm Center

The Advanced Cyber Security Center

CERT

The National Vulnerability Database website

#### Feedback

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.

The correct answer is: The National Vulnerability Database website

### Question 14

Incorrect

Mark 0.00 out of 2.00

Flag question

#### Question text

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?

Select one:

CVE national database

ISO/IEC 27000 model

Infragard

NIST/NICE framework

#### Feedback

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.

The correct answer is: CVE national database

### Question 15

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

digital signature

digital certificate

asymmetric encryption

salting

#### Feedback

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.

The correct answer is: digital certificate

### Question 16

Incorrect

Mark 0.00 out of 2.00

Flag question

#### Question text

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

Select one:

the public key of Bob

the private key of Bob

the private key of Alice

the public key of Alice

#### Feedback

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.

The correct answer is: the public key of Bob

### Question 17

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

Local Security Policy tool

Computer Management

Event Viewer security log

Active Directory Security tool

#### Feedback

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.

The correct answer is: Local Security Policy tool

### Question 18

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

A user has a large amount of data that needs to be kept confidential. Which algorithm would best meet this requirement?

Select one:

RSA

Diffie-Hellman

3DES

ECC

#### 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: 3DES

### Question 19

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

spam

browser hijacker

DNS poisoning

SEO poisoning

#### Feedback

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.

The correct answer is: SEO poisoning

### Question 20

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

MS Baseliner

SANS Baselining System (SBS)

CVE Baseline Analyzer

Microsoft Security Baseline Analyzer

#### Feedback

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

The correct answer is: Microsoft Security Baseline Analyzer

What approach to availability involves using file permissions?

Select one:

layering

obscurity

simplicity

limiting

#### Feedback

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.

The correct answer is: limiting

### Question 22

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 front office of a major league sports team

the U.S. Department of Education

the New York Stock Exchange

#### 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

### Question 23

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

What technique creates different hashes for the same password?

Select one:

HMAC

salting

SHA-256

CRC

#### Feedback

Refer to curriculum topic: 5.1.2  
Data integrity is one of the three guiding security principles. A cybersecurity specialist should be familiar with the tools and technologies used ensure data integrity.

The correct answer is: salting

### Question 24

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:

802.11i

802.11q

TKIP

WPA2

WEP

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 25

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Keeping data backups offsite is an example of which type of disaster recovery control?

Select one:

preventive

detective

corrective

management

#### Feedback

Refer to curriculum topic: 6.4.1  
A disaster recovery plan enables an organization to prepare for potential disasters and minimize the resulting downtime.

The correct answer is: preventive

### Question 26

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

a biometric fingerprint reader

a set of attributes that describes user access rights

observations to be provided to all employees

user login auditing

#### Feedback

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.

The correct answer is: a set of attributes that describes user access rights

### Question 27

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

An organization just completed a security audit. Your division was cited for not conforming to X.509 requirements. What is the first security control you need to examine?

Select one:

digital certificates

data validation rules

VPNs and encryption services

hashing operations

#### Feedback

Refer to curriculum topic: 5.3.2  
Digital certificates protect the parties involved in secure communications.

The correct answer is: digital certificates

### Question 28

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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.)

Select one or more:

They increase processing requirements.

They require more equipment.

They contain personal information.

They collect sensitive information.

They make systems more complicated.

They require 24-hour monitoring.

#### Feedback

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

The correct answers are: They collect sensitive information., They contain personal information.

### Question 29

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

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

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

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

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

#### Feedback

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

The correct answer is: a validation rule which has been implemented to ensure completeness, accuracy, and consistency of data

### Question 30

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

technologies, policies, and awareness

confidentiality, integrity, and availability

secrecy, identify, and nonrepudiation

encryption, authentication, and identification

#### Feedback

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

The correct answer is: confidentiality, integrity, and availability

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

Select one or more:

STP

RIP

WPA2

ICMP

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 32

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which hashing technology requires keys to be exchanged?

Select one:

salting

HMAC

MD5

AES

#### Feedback

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

The correct answer is: HMAC

### Question 33

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one or more:

data in-process

data in-transit

purged data

stored data

data encrypted

data decrypted

#### Feedback

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.

The correct answers are: stored data, data in-transit, data in-process

### Question 34

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

trusted partners

familiarity

urgency

intimidation

#### Feedback

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

The correct answer is: intimidation

### Question 35

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:

improving reliability and uptime of the servers

stronger encryption systems

remote access to thousands of external users

limiting access to the data on these systems

#### 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 36

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

asset standardization

asset identification

asset classification

asset availability

#### Feedback

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.

The correct answer is: asset standardization

### Question 37

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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)

Select one or more:

rainbow tables

password digest

lookup tables

rouge access points

reverse lookup tables

algorithm tables

#### Feedback

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

The correct answers are: rainbow tables, lookup tables, reverse lookup tables

### Question 38

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which cybersecurity weapon scans for use of default passwords, missing patches, open ports, misconfigurations, and active IP addresses?

Select one:

packet sniffers

vulnerability scanners

password crackers

packet analyzers

#### Feedback

Refer to curriculum topic: 8.2.4  
There are many tools that a cybersecurity specialist uses to evaluate the potential vulnerabilities of an organization.

The correct answer is: vulnerability scanners

### Question 39

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Users report that the network access is slow. After questioning the employees, the network administrator learned that one employee downloaded a third-party scanning program for the printer. What type of malware might be introduced that causes slow performance of the network?

Select one:

phishing

virus

spam

worm

#### 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: worm

### Question 40

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

Look for usernames that do not have passwords.

Look for policy changes in Event Viewer.

Look for unauthorized accounts.

Scan the systems for viruses.

#### 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: Look for unauthorized accounts.

Before data is sent out for analysis, which technique can be used to replace sensitive data in nonproduction environments to protect the underlying information?

Select one:

steganography

steganalysis

software obfuscation

data masking substitution

#### Feedback

Refer to curriculum topic: 4.3.1  
Technologies exist to confuse attackers by changing data and using techniques to hide the original data.

The correct answer is: data masking substitution

### Question 42

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

A cybersecurity specialist is asked to identify the potential criminals known to attack the organization. Which type of hackers would the cybersecurity specialist be least concerned with?

Select one:

white hat hackers

gray hat hackers

black hat hackers

script kiddies

#### Feedback

Refer to curriculum topic: 1.2.1  
Hackers are classified by colors to help define the purpose of their break-in activities.

The correct answer is: white hat hackers

### Question 43

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

mitigation and acceptance

confidentiality and eradication

detection and analysis

risk analysis and high availability

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 44

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

rate of false positives and rate of acceptability

rate of acceptability and rate of false negatives

rate of rejection and rate of false negatives

rate of false negatives and rate of false positives

#### Feedback

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.

The correct answer is: rate of false negatives and rate of false positives

### Question 45

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

It prevents casual trespassers because of its height.

It deters casual trespassers only.

The fence deters determined intruders.

It offers limited delay to a determined intruder.

#### Feedback

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

The correct answer is: It deters casual trespassers only.

### Question 46

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

In which situation would a detective control be warranted?

Select one:

when the organization needs to look for prohibited activity

when the organization needs to repair damage

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

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

#### Feedback

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.

The correct answer is: when the organization needs to look for prohibited activity

### Question 47

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

Keyspace increases exponentially.

Keyspace decreases exponentially.

Keyspace decreases proportionally.

Keyspace increases proportionally.

#### 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: Keyspace increases exponentially.

### Question 48

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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

Select one:

Gramm-Leach-Bliley Act

Sarbanes-Oxley Act

The Federal Information Security Management Act

Import/Export Encryption Act

#### Feedback

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

The correct answer is: Sarbanes-Oxley Act

### Question 49

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

Which access control should the IT department use to restore a system back to its normal state?

Select one:

compensative

detective

corrective

preventive

#### Feedback

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.

The correct answer is: corrective

### Question 50

Correct

Mark 2.00 out of 2.00

Flag question

#### Question text

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?

Select one:

man-in-the-middle

DoS

SQL injection

packet Injection

#### 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: DoS