Question 1: Skipped

Which access control model assigns users to predefined roles and grants permissions based on their job responsibilities?

RBAC	(Correct)
O MAC	
ABAC	
O DAC	

Role-based access control (RBAC) assigns users to predefined roles and grants permissions based on their job responsibilities. RBAC simplifies access control management by organizing users into roles and assigning permissions to each role, rather than assigning permissions to each user. RBAC is suitable for environments where users have well-defined job responsibilities.

Question 2:	Skipped	
Which of th	ese is an example	of deterent control?
	turnstile	
	encryption	
	guard-dog	(Correct)

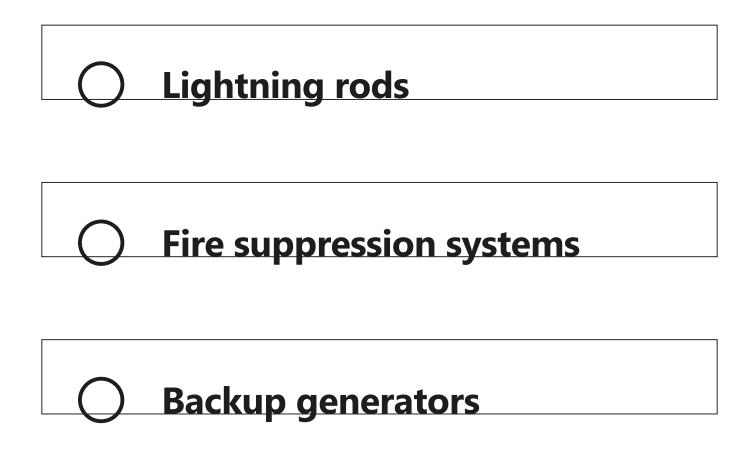


Deterrent controls are a type of security measure designed to deter or discourage unauthorized access or behavior. They are intended to make it more difficult or risky for an attacker to attempt to gain unauthorized access to a resource or system. Examples of deterrent controls include security cameras, motion sensors, alarms, warning signs, and guard dogs.

Question 3: Skipped

A company needs to protect its critical infrastructure from natural disasters. Which physical control is best suited for this scenario?





Flood barriers are best suited for protecting critical infrastructure from natural disasters such as floods. They prevent water from entering the building and damaging critical equipment.

Question 4: Skipped

Which of the following is an example of a technical access control?

A guard at the entrance to a building

A policy that defines the rules for assigning access to authorized individuals

A firewall that separates untrusted networks from trusted networks

(Correct)



A firewall is technical access control. Locks and Guards are physical access controls while policies are administrative access controls

Question 5: **Skipped**

Tesmo Inc is looking for controlling and preventing the spread of malware and viruses, what type of control can be used?



Technical control (Correct)

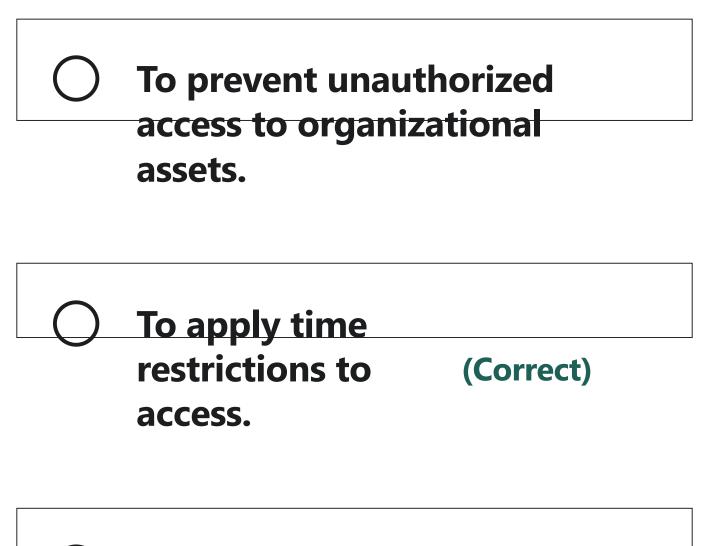


Logical controls are used to prevent the spread of malware and viruses. Examples of logical controls include antivirus software intrusion detection and prevention systems and firewalls.

Question 6: Skipped

What is the primary purpose of time-based access?

To validate the level of access a user should have to a file.



To manage business continuity and disaster recovery plans.

Explanation

Time-based access control is a security mechanism that restricts access to a resource or system based on the time of day, week, month, or year. This mechanism allows administrators to define specific time windows during which users are permitted or denied access to a particular system or resource.

Question 7:	Skipped
-------------	---------

Profit inc after suffering a data breach has hired Gloria. What control should Gloria implement in order to prevent from any future data breach?

O Physical control	
Administrative control	
Rule-based access control	

Logical control (Correct)

Logical controls are used to prevent data breaches by limiting the amount of data that users can access. Examples of logical controls include access controls permissions and data classification.

Question 8: Skipped

What is the primary difference between a subject and an object?



A subject
initiates a
request for
access, while an (Correct)
object is the
target of the
request

There is no difference between a subject and an object

A subject controls access to resources, while an object requests access to services

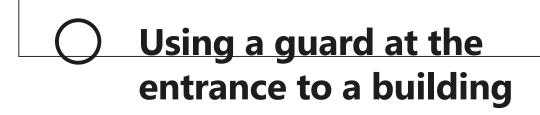
A subject initiates a request for access, while an object is the target of the request. In access control, a subject is an entity that can perform actions on objects, such as accessing a resource or modifying data.

Question 9: Skipped

Which of the following is an example of administrative control? (\star)

Using a lock on the door to a data center

Using a firewall to separate untrusted networks from trusted networks



Using a policy
that defines the
rules for
assigning access
to authorized
individuals

(Correct)

Explanation

an administrative control is a policy that defines the rules that assign access to authorized individuals, and gives an example of a policy being used as a layer of defense in depth to prevent unauthorized access to data in a data center.

Question 10: Skipped

policy de	cision point (i bi).	
	DAC	
	ABAC	(Correct)
	RBAC	
	MAC	

Which access control method uses attributes and rules

to define access policies that are evaluated by a central

nolicy decision point (PDP)?

Explanation

Attribute-based access control (ABAC) uses attributes and rules to define access policies that are evaluated by a central policy decision point (PDP). ABAC provides fine-

grained access control by using multiple attributes to determine whether to grant access or not. ABAC is suitable for environments with dynamic access requirements.

Question 11: Skipped

A company needs to ensure that its employees can access the network resources only from authorized devices. Which logical control is best suited for this scenario?

0	Antivirus software
	Encryption
	Access controls

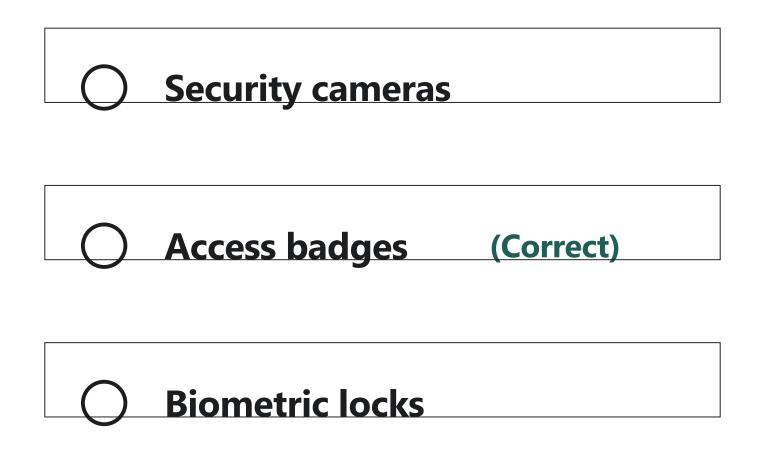


Network access control (NAC) is best suited for this scenario. NAC ensures that only authorized devices can access the network resources by checking the device's security posture and enforcing security policies.

Question 12: Skipped

A company wants to prevent unauthorized access to its server room. Which physical control is best suited for this scenario?





Access badges are best suited for this scenario. They allow for easy identification of authorized personnel and restrict access to the server room to those with valid badges.

Question 13: Skipped

Which of the following access control model assigns security labels to data and enforces access based on the sensitivity of the data and the clearance of the user?

ABAC (Attribute based access control)
Bell-LaPadula (Correct)
DAC (Discretionary Access Control)
MAC (Mandatory Access

Bell-LaPadula (BLP) is a mandatory access control (MAC) model that assigns security labels to data and enforces access based on the sensitivity of the data and the

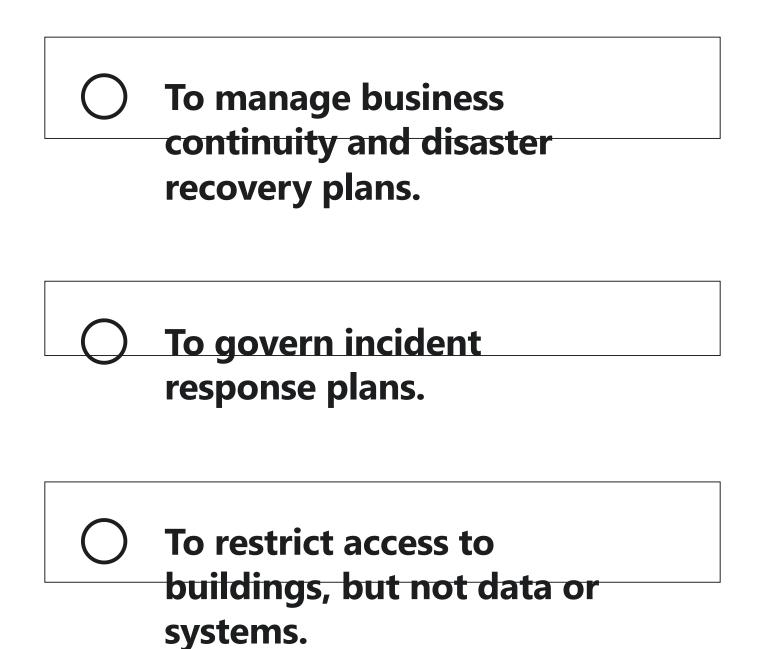
clearance of the user. BLP prevents information flow from high-security levels to lower-security levels, but it allows read-only access from lower-security levels to highersecurity levels.

Question 14: Skipped

Linda works for a large organization that has multiple systems and applications. The organization decides to implement an integrated identity and access management system. What would be the main purpose of this system?

To prevent
unauthorized
access to
organizational
assets.

(Correct)



The system would help to streamline the management of user identities and access permissions across all of the organization's systems and applications, reducing the risk of security breaches caused by unauthorized access or user error.

Question 15: Skipped

Which of the following is an example of a communications resource?

	A network (Correct) protocol
	An object owner
0	A user password
	An access control rule

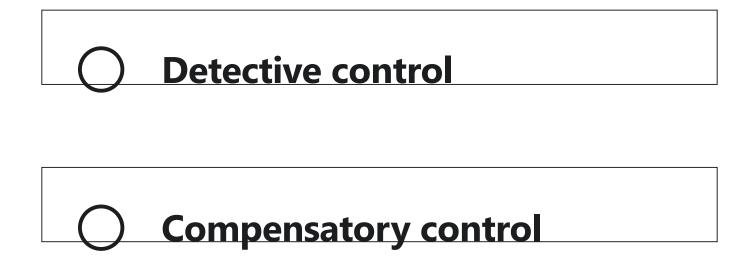
In the context of information technology, a communications resource refers to any hardware, software, or protocol that is used to facilitate the exchange of information or data between two or more entities, such as devices, applications, or networks. Examples of communications resources include protocols, such as TCP/IP, HTTP, SMTP, and FTP

Question 16: Skipped

Which type of control is used to restore systems or processes to their normal state after an attack has occurred?

Recovery control
Recovery control



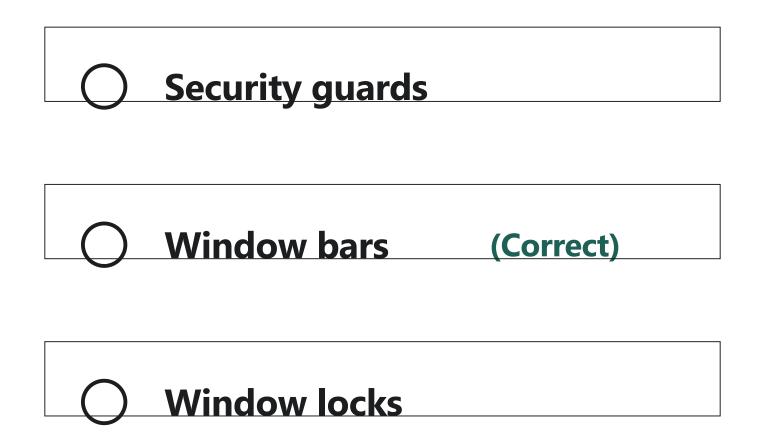


Corrective controls are used to restore systems or processes to their normal state after an attack has occurred. Examples of corrective controls include virus removal tools data recovery software and system restoration procedures.

Question 17: Skipped

Which physical control is used to protect a building from unauthorized access through its windows?





Window bars are used to protect a building from unauthorized access through its windows. They prevent intruders from breaking into the building by blocking access to the windows.

Question 18: Skipped

Which access control model grants permissions based on the sensitivity of the data and the user's job function?

0	DAC	
0	MAC	
	Rule-based ad (RBAC2)	ccess control
	RBAC	(Correct)

In RBAC, access permissions are granted based on the role or job function of the user and the sensitivity of the data or resource being accessed. Access is granted based on predefined roles or job functions, and users are assigned to those roles based on their job responsibilities and clearance levels.

Question 19: Skipped

What is the main problem with assigning static privileges to administrative users on a database?

- Security is

 dependent upon
 the login
 process

 (Correct)
 - Administrative users may forget their privileges
 - Static privileges may not provide enough access

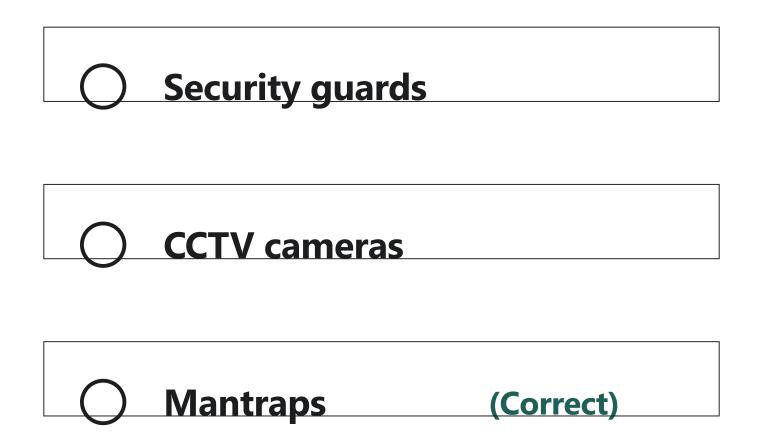


The passage states that without privileged access management, the system's access control would have those privileges assigned to the administrative user in a static way effectively "on" 24 hours a day every day making security dependent upon the login process.

Question 20: Skipped

Which of the following physical controls is used to protect a building from unauthorized access and monitor the movement of people?

F		
<u>Fences</u>		



Mantraps are used to protect a building from unauthorized access and monitor the movement of people. A mantrap is a small space between two doors, where the first door must be closed and locked before the second door can be opened.

Question 21: Skipped

ANSE.co enterprise has strict restrictions on the access of computer systems and data, which controls are they using?

Administrative control			
Logical control (Correct)			
O Physical control			
Social control			

Logical controls are used to restrict access to computer systems and data. Examples of logical controls include passwords access controls firewalls and intrusion detection systems.

Question 22: Skipped

What is the purpose of comparing multiple attributes in an access rule?

- To apply time-based access.
 - To determine

 appropriate
 access to an object.

 (Correct)
 - To deny access to an object.

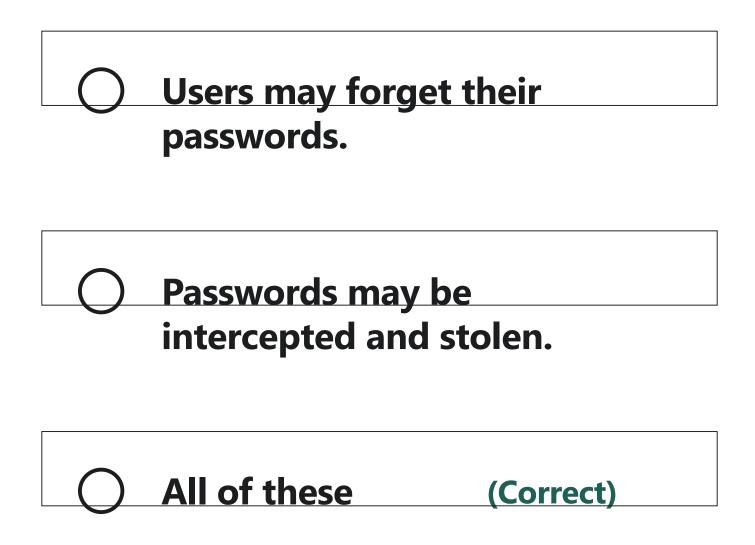


Access rules are a fundamental component of access control, which is the process of granting or denying access to a resource or system. An access rule typically consists of one or more conditions or attributes that are used to determine whether a particular user or entity is authorized to access a particular resource or system.

Question 23: Skipped

A company has implemented a system that requires users to provide a username and password to access its resources. Which of the following is a weakness of this authentication method?





The weakness of the username and password authentication method is that users may forget their passwords, share their passwords with others or have their passwords intercepted and stolen by attackers.

Question 24: Skipped

The management of Dmardoc Pvt Ltd has decided to place controls to protect against environmental threats such as fire, flood and earthquakes, what controls are they considering?

Logical control
Administrative control
Physical control (Correct)
Technical control

Explanation

Physical controls are used to protect against environmental threats such as fire flood and earthquakes. Examples of

physical controls include fire suppression systems flood barriers and seismic detectors.

Question	25:	Skippe	

A company wants to ensure that its employees can only access the resources they need to perform their job functions. Which access control model is best suited for this scenario?

DAC	
MAC	
RBAC	(Correct)
ABAC	

Role-based access control (RBAC) is best suited for this scenario. RBAC assigns users to predefined roles and grants permissions based on their job responsibilities.

Question 26: Skipped

A company wants to ensure that its employees can evacuate the building in case of an emergency. Which physical control is best suited for this scenario?

Emergency lighting	
Exit signs	
Fire alarms	



Emergency exit doors are best suited for ensuring that employees can evacuate the building in case of an emergency. They provide a safe and quick exit route and are designed to open easily in case of an emergency.

Question 27: Skipped

A new BYOD policy has been enforced in Retaw Insurance Group, which type of control is used to enforce this security policy?



Administrative control	(Correct)
Operational conti	rol
Logical control	

Administrative controls are used to enforce security policies and procedures. Examples of administrative controls include security policies procedures standards and guidelines.

Question 28: Skipped

What is the purpose of defense in depth in information security?

	To guarantee that a cyberattack will not occur
0	To establish variable barriers
	across multiple (Correct) layers and missions of the organization
0	To implement only technical controls to prevent a cyberattack
0	To provide unrestricted access to organizational

assets

Explanation

defense in depth is an information security strategy that integrates people, technology and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Question 29: Skipped

Which of the following is an example of an access control list? (*)







A user's password

Explanation

An access control list (ACL) is a list of rules that determines which users or entities are authorized to access a particular resource or system. ACLs can be implemented at various levels, including network, application, and file system.

Question 30: Skipped

Dennis working for Malleys food needs to prevent unauthorized access to data and systems by managing user accounts and privileges. What type of control is needed to accomplish this?

Administrative (Correct)
Operational control
Physical control
Logical control

Administrative controls are used to prevent unauthorized access to data and systems by managing user accounts and privileges. Examples of administrative controls include access controls identity and access management (IAM) systems and security policies and procedures.

Question 31: Skipped

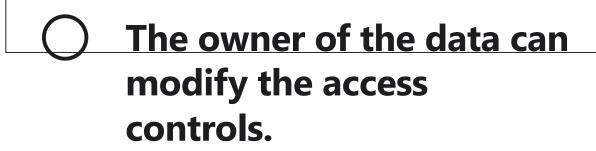
A company has implemented mandatory access control (MAC) for its confidential data. Which of the following statements is true?

Access controls

cannot be
changed by
anyone except
the system
administrator.

(Correct)

The data can be accessed by users who possess a need-to-know.



The system administrator can change the access controls.

Explanation

Mandatory access control is a type of access control system that restricts access to resources based on security labels assigned to each resource and each user. In a MAC system, the security labels are predefined and cannot be modified by users. The system administrator is responsible for assigning security labels to resources and users, and for configuring the access control policies that enforce the security labels.

Question 32: Skipped

Which of the following can be done to limit the damage caused by the ransomware attack?

- Limit the use of
 administrator
 privileges to (Correct)
 only when
 required
 - Add more administrative
 users to the Domain
 Admins group

O Delete all emails with attachments



Use a different email client to prevent malicious attachments

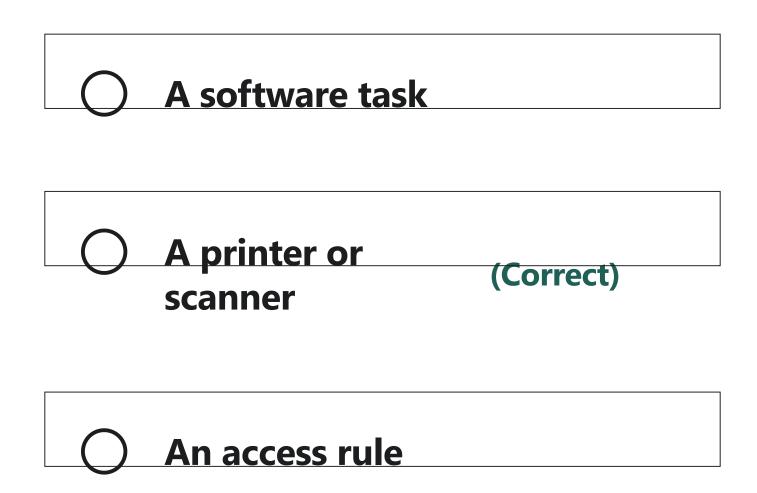
Explanation

The passage states that a privileged access management solution could limit the damage done by the ransomware if the administrator privileges are only used when performing a function requiring that level of access, such as performing routine operations without a higher level of access.

Question 33: Skipped

Which of the following is an example of a device?





In the context of information technology, a device refers to any physical or virtual component or peripheral that is used to perform a specific function or task. Examples of devices include printers, scanners, keyboards, mice, monitors, hard drives, routers, and switches.

Question 34: Skipped

A company wants to ensure that its employees can access network resources from anywhere in the world. Which access control model is best suited for this scenario? (*)

MAC	
RBAC	
ABAC	(Correct)
O DAC	

Explanation

Attribute-based access control (ABAC) is best suited for this scenario. ABAC uses attributes such as user identity location and device type to determine access to network resources.

Question 35: Skipped

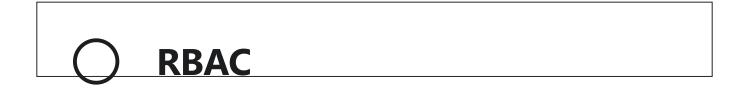
Lighting

A company wants to protect its parking lot from theft and vandalism. Which physical control is best suited for this scenario?

	Security cameras (Correct)
0	Perimeter fencing
0	Security guards

Security cameras are best suited for protecting a parking lot from theft and vandalism. They allow for continuous monitoring of the area and can deter criminals from committing crimes.

Question 36: Skipped	
What type of access control system uses a user's physical characteristics to authenticate their identity?	
O ACL	
Biometric	(Correct)
MAC	



Unlike traditional authentication methods such as passwords, smart cards, or tokens biometric authentication relies on the physical characteristics of the user such as fingerprint facial recognition or iris recognition.

Question 37: Skipped

Which of the following is an example of a subject? (★)



A printer or scanner



In computer security and access control, a subject is an entity that can perform actions on objects, such as accessing a resource or modifying data. An authorized user is a specific type of subject that has been granted permission to access certain resources or perform certain actions within a system.

Question 38: Skipped

What is the primary purpose of access controls in information security?

0	To allow or deny
	access to (Correct) assets
	To govern incident response plans
0	To manage business continuity and disaster recovery plans
0	To restrict access to buildings, but not data or systems

Γ

Access controls are used to ensure that only authorized users are able to access sensitive information or systems within an organization, while also preventing unauthorized access and potential data breaches

Question 39: Skipped

A company wants to prevent unauthorized access to its systems by limiting access to specific IP addresses. Which logical control is best suited for this scenario?

Access conf	trols
Encryption	
Firewalls	(Correct)



Firewalls are best suited for preventing unauthorized access to systems by limiting access to specific IP addresses. Firewalls allow or block traffic based on predefined rules and policies.

Question 40: Skipped

A company uses multifactor authentication (MFA) to protect its resources. Which of the following is an example of something the user has in MFA?



Smart card	(Correct)
Username an	d password
Fingerprint	

A smart card is an example of something the user has in multifactor authentication (MFA). Other examples of something the user has include a USB token, a security token, or a one-time password (OTP) generator.

Question 41: Skipped

What is an access rule?

Anything that a subject attempts to access.

An entity that requests access to organizational assets.

An access rule is an instruction developed to allow or deny access to an object by comparing the validated identity of the

subject to an

(Correct)

access control list.



Explanation

An access rule is an instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list. In access control, an access rule is used to define the specific conditions under which a subject is authorized to access an object. The access rule compares the identity of the subject to an access control list (ACL) that specifies the access permissions for the object.

Question 42: Skipped

A security administrator needs to configure a system to prevent users from logging in outside of their normal business hours. Which access control model is best suited for this scenario?

MAC	
Time-based access control (TBAC)	(Correct)
RBAC	
DAC	

Time-based access control (TBAC) is the best access control model for this scenario. TBAC enforces access controls based on the time of day, day of the week, or other time-related criteria.

Question 43: Skipped

Which of the following is an example of a process?

- O An input/output port.
 - A software task. (Correct)

A communications resource.

A printer or scanner.

In the context of information technology, a process refers to an executing program or software task that performs a specific function or set of functions. A process can be a standalone program, a module within a larger program, or a set of interdependent programs that work together to achieve a particular goal.

Question 44: Skipped

Which type of control is used to identify that an attack has occurred or is currently occurring?

Preventive control	
Detective (Correct)	
control (Correct)	

Recovery control



Detective controls are used to identify that an attack has occurred or is currently occurring. Examples of detective controls include intrusion detection systems security logs and security audits.

Question 45: Skipped

Which of the following is an example of an object?



A network protocol

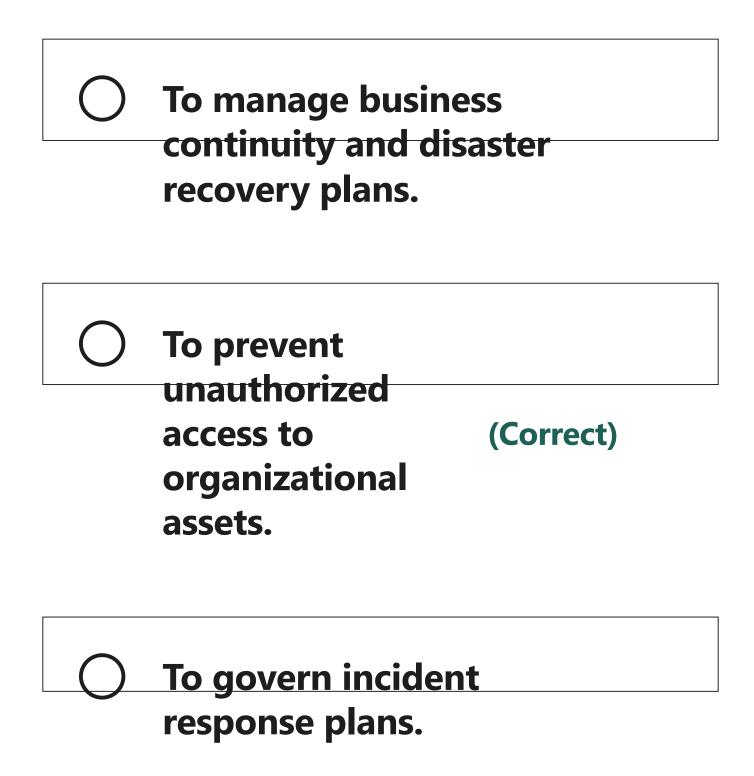


an object is a resource or asset that is being protected, such as data, files, programs, devices, or systems.

Question 46: Skipped

What is the primary purpose of denying access to unauthorized functions or individuals?





Access control is the process of granting or denying access to resources based on an entity's identity, role, or other attributes. By denying access to unauthorized functions or individuals, organizations can prevent unauthorized access or misuse of sensitive or confidential information and protect their assets from potential security breaches.

Question 47: Skipped

Which of the following is an example of multi-factor authentication?

Using a policy to assign access to authorized individuals

Using a username and password

Using a firewall to separate untrusted

networks from trusted networks

Using a code

sent to your
phone to verify
your identity

(Correct)

Explanation

technical example of defense in depth is multi-factor authentication, in which multiple layers of technical controls are implemented, such as using a username and password followed by a code sent to your phone to verify your identity.

Question 48: Skipped

In order to ensure that access to organizational assets is controlled and monitored, the CIO decide to implement

rule base?	
	To apply time-based access.
	To define how
	much access is (Correct) allowed.
	To provide service to a
_	user.
	To record the rules of
	access to an object.

a rule base. What would be the primary purpose of this

A rule base is a set of rules that is used to control access to organizational assets. The rule base specifies the access permissions that are granted to a subject (such as a user or group) for a specific object.

Question 49: Skipped

A company needs to ensure that its employees can access the network resources from anywhere in the world. Which access control process is best suited for this scenario?

Authentication (Correct)

Authorization

Identification



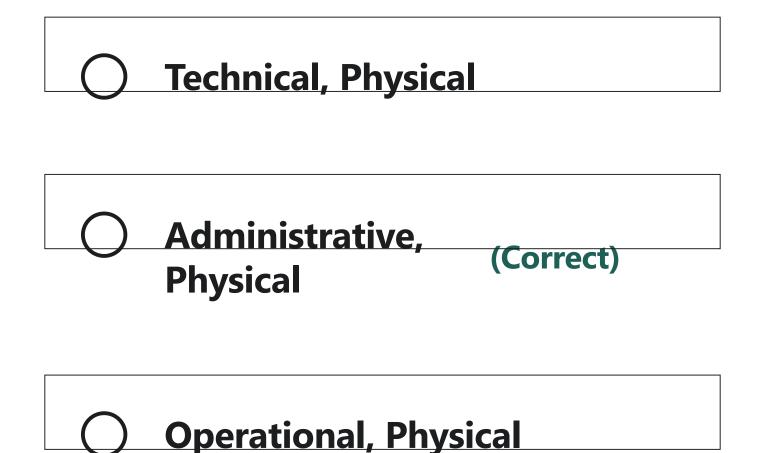
Authentication is best suited for this scenario.

Authentication verifies the identity of the user and grants access to the network resources based on the user's credentials.

Question 50: Skipped

An organization wants to restrict employee after-hours access to its systems so it publishes a policy forbidding employees to work outside of their assigned hours, and then makes sure the office doors remain locked on weekends. This is an example of:





Administrative controls are security measures that rely on administrative or procedural policies and practices to manage and reduce risk. In the scenario, the organization is implementing an administrative control by publishing a policy that forbids employees from working outside of their assigned hours. Physical controls, on the other hand, are security measures that are implemented to physically prevent unauthorized access to a resource or system. In the scenario, the organization is implementing a physical control by locking the office doors on weekends to prevent unauthorized access to its systems. By implementing a

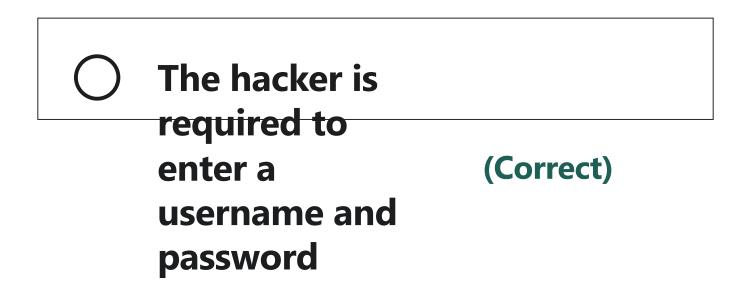
combination of administrative and physical controls, the organization can effectively reduce the risk of unauthorized access to its systems after-hours.

Question 51: Skipped

A hacker is trying to gain access to a company's network. Which of the following scenarios would be an example of defense in depth?

The company relies solely on a firewall to block unauthorized access

The company stores all sensitive data on a single server



O None of these

Explanation

it describes a layered defense strategy using multiple countermeasures, making it more difficult for the hacker to gain access. Using a firewall solely is incorrect as it describes only a single technical control. Storing data on a single server is incorrect as storing all sensitive data on a single server is not an example of defense in depth.

Question 52: Skipped

Which access control model is best suited for a large organization with many departments that have different data access needs?

RBAC	(Correct)
DAC	
MAC	
○ ACL	

Explanation

Role-based access control (RBAC) is best suited for a large organization with many departments that have different data access needs. RBAC simplifies access control

management by organizing users into roles and assigning permissions to each role, rather than assigning permissions to each user.

Question 53: Skipped

systems

A company needs to protect its confidential data from unauthorized access. Which logical control is best suited for this scenario?

<u> </u>	ncryption	(Correct)
F	irewalls	
	ntrusion dete	ction



Encryption is best suited for protecting confidential data from unauthorized access. Encryption ensures that data is protected by making it unreadable without the appropriate decryption key.

Question 54: Skipped

A company wants to ensure that its employees cannot bring unauthorized electronic devices into the workplace. Which physical control is best suited for this scenario? (*



O RFID scanners



Metal detectors are the physical control that is best suited for preventing employees from bringing unauthorized electronic devices into the workplace. Metal detectors are commonly used to screen individuals and their belongings for metal objects, including electronic devices. Metal detectors can be placed at entry and exit points to a workplace to detect metal objects on an individual's person or in their bags or belongings.

Question 55: Skipped

Which of the following situations call for provisioning new user accounts and changing privileges?

0	When a company wants to reduce an employee's access privileges.
	When a company wants to promote an employee
	When an employee is (Correct) hired
	When an employee has left the company

ı

provisioning new user accounts is required when an employee is hired. "When a company wants to promote an employee" is incorrect as it describes a change to an employee's role rather than the creation of a new account. "When an employee has left the company" is incorrect as it describes disabling accounts after

Question 56: Skipped

A company wants to ensure that its employees can access the data center only during business hours. Which access control concept is best suited for this scenario?



Least privilege





Time-based access control (TBAC) is best suited for this scenario. TBAC restricts access to resources based on the time of day limiting access to the data center to business hours.

Question 57: Skipped

What is the purpose of granting appropriate levels of access to authorized personnel and processes?

	To restrict access to organizational assets.
	To govern incident response plans.
0	To manage business continuity and disaster recovery plans.



To ensure that authorized

personnel and processes can access services and resources.

(Correct)

Explanation

The purpose of granting appropriate levels of access to authorized personnel and processes is to ensure that they can access services and resources necessary to perform their job functions or tasks, while also protecting sensitive or confidential information.

Question 58: Skipped

Which type of control is used to minimize the impact of an attack and to restore normal operations as quickly as possible?

Compensatory control
Corrective control
Recovery control (Correct)
Detective control

Recovery controls are used to minimize the impact of an attack and to restore normal operations as quickly as possible. Examples of recovery controls include backup systems disaster recovery plans and business continuity plans.

Question 59: Skipped

Which of the following physical controls is used to protect against eavesdropping and data theft through electromagnetic radiation?

Screening rooms
EMI shielding (Correct)
White noise generators
None of these

EMI shielding is the physical control used to protect against eavesdropping and data theft through electromagnetic radiation.

Question 60: Skipped

Mathew's workplace is reviewing its access control procedures and considering implementing either just-in-time privileged access management or static access management. However, the team is unsure about the difference between these two approaches. How should mathew explain the distinction between just-in-time privileged access management and static access management?

Static access management limits the amount of access available to administrative users

Just-in-time privileged access management assigns role-based specific subsets of privileges that only become active in real-

time

(Correct)

Just-in-time privileged

access management
assigns privileges to
administrative users in a
static way



Static access management can prevent ransomware attacks

Explanation

The passage states that just-in-time privileged access management includes role-based specific subsets of privileges that only become active in real time when the identity is requesting the use of a resource or service, as opposed to being assigned in a static way.