Question 1:	Skipped		
What is an example of a symmetric encryption technique?			
	Public key encryptic	on	
	Substitution cipher	(Correct)	
	RSA encryption		
	Diffie-Hellman key		

A substitution cipher is an example of a symmetric encryption technique where each letter of the plaintext is replaced with another letter or bit.

Question	2: <b>Skipped</b>		
Which of the following devices is best suited for ingress monitoring in a large enterprise			
	Router		
	Intrusion		
	detection system (IDS)	(Correct)	
	Firewall		



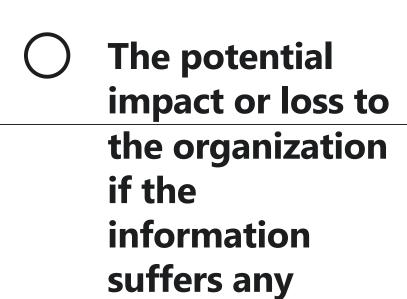
An intrusion detection system (IDS) is best suited for ingress monitoring in a large enterprise network because it is designed specifically to detect and alert on suspicious activity, making option d the correct answer.

Question 3: Skipped

A company is unsure about how to classify their data. What should they assess before assigning labels?



The number of users who access the data



(Correct)

The data format

compromises

security

# **Explanation**

Before any labels can be attached to sets of data that indicate its sensitivity or handling requirements, the potential impact or loss to the organization needs to be assessed.

#### Question 4: Skipped

A company is concerned about its data being shared without its authorization. Which stage in the data life cycle would be most effective to implement access controls?

<b>Storing</b>	
<b>Creating</b>	
Sharing	(Correct)
( ) Using	

The data life cycle includes the stages of creating, storing, using, sharing, and disposing of data. Each stage of the data life cycle presents different risks and opportunities for implementing security controls. In the context of data sharing, access controls are most effective when implemented at the sharing stage. This is because it is at the sharing stage that data is most vulnerable to being shared without authorization.

Question 5: Skipped

What is the purpose of purging a device or system?

To physically destroy the device or system

To wipe the device or system



To eliminate or greatly reduce the chance that residual physical effects from the writing of the original data values may still be recovered

(Correct)

#### **Explanation**

Purging the device or system eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered.

Question 6: Skipped

What activities might need to be completed for a change rollback?

Implementing the change

Scheduling the change

Evaluating the change

All of the above (Correct)

#### **Explanation**

Depending upon the nature of the change a variety of activities may need to be completed for a change rollback including scheduling the change testing the change verifying the rollback procedures implementing the change evaluating the change for proper and effective operation and documenting the change in the production environment.

Question 7: Skipped

What is the process of clearing a device or system?

O Writing multiple
patterns of
random values (Correct)
throughout all
storage media

Destroying the device or system





Clearing the device or system usually involves writing multiple patterns of random values throughout all storage media.

Question 8: Skipped

How does asymmetric encryption provide confidentiality?

0	By using the same key for encryption but different keys for decryption	
	By not involving any keys	
0	By using different keys for encryption and decryption	
	By using the same key for encryption and decryption	

Γ

Asymmetric encryption provides confidentiality by using different keys for encryption and decryption. The sender encrypts the message with the public key of the receiver, and only the receiver with the private key can open or read the message.

Question 9: Skipped

An organization wants to keep track of changes to their data over time. Which stage in the data life cycle model involves modifying the data?

<b>Creating</b>	
<b>Using</b>	(Correct)
Storing	

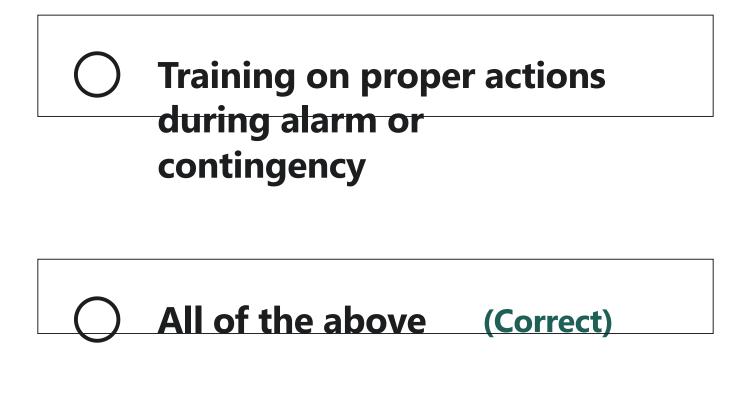


Using the knowledge, which may cause the information to be modified, supplemented or partially deleted, is the stage where changes to data are made.

Question 10: Skipped

What is an example of security awareness training in fire safety?







An example of security awareness training in fire safety includes educating workers on the interaction of fire and smoke detectors, training them on the proper actions to take during an alarm or contingency, and posting signage and floor markings to constantly remind workers of what to do. Similarly, in an anti-phishing campaign, education can help users understand how social engineering attacks are conducted, training can help increase proficiency in

recognizing and responding to phishing attempts, and awareness can raise overall awareness of the threat posed by phishing attacks and alert users to new tactics.

Question 11: Skipped

What is the first step in the classification process?

O Documenting retention requirements for the data

O Destroying data that is no longer in use

Assigning labels that indicate the sensitivity or handling requirements of the data



Assessing the potential impact

or loss to the organization if the information suffers any security compromises

(Correct)

# **Explanation**

Before any labels can be attached to sets of data that indicate its sensitivity or handling requirements, the potential impact or loss to the organization needs to be assessed.

Question 12: Skipped

What is the data security life cycle model useful for?

- Understanding the life cycle of software components
  - Understanding the life cycle of hardware components

Aligning easily with the different roles that people and organizations perform during the evolution of

data

(Correct)



The data security life cycle model is useful because it can align easily with the different roles that people and organizations perform during the evolution of data from creation to destruction (or disposal).

Question 13: Skipped

What could happen if data labeled as "highly restricted" is compromised?



It could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities.

It could possibly put the organization's future existence at risk.
Compromise could lead to substantial loss of life, injury or property

damage, and the

litigation and

(Correct)

# claims that would follow.

O It would have no impact.

#### **Explanation**

Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow.

Question 14: Skipped

What is the purpose of a data retention policy?



0	To ensure that no data is kept	
	beyond its (Correct) required or useful life	
	To encrypt data during	
	transmission	
0	To ensure that data is stored in a secure location	

Data retention policies are applicable both for hard copies and for electronic data, and no data should be kept beyond its required or useful life. Question 15: Skipped

An organization is getting rid of old hard drives. What should they do to protect sensitive information on these drives?

- **Encrypt the drives** 
  - Keep the drives in storage

O Purge the drives
or physically (Correct)
destroy them



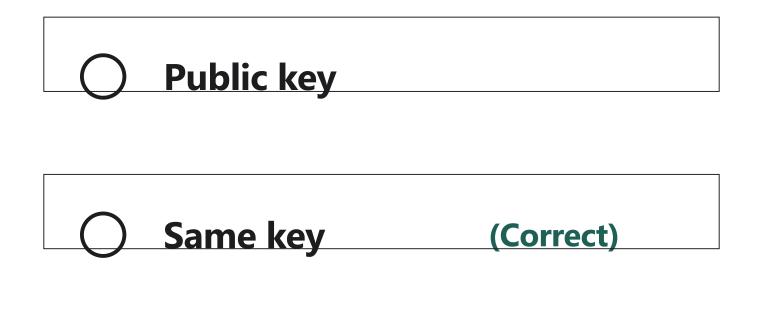
When system elements are to be removed and replaced, either as part of maintenance upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.

Question 16: Skipped

What is another name for symmetric algorithms?

( )	Private kev	

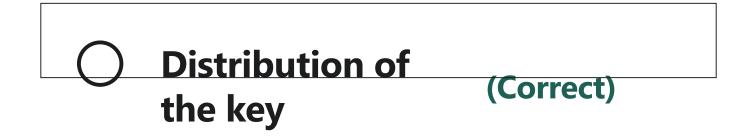
**Encryption key** 



Symmetric algorithms may also be referred to as same key, single key, shared key, secret key or session key.

Question 17: Skipped

What is a challenge of using symmetric encryption?



Key management
Data availability
Message integrity

Sharing the key can be challenging because it cannot be sent through the same channel as the encrypted message or the MITM would have access to it.

Question 18: Skipped

A company is looking to improve their data security practices. What process can they implement to reduce the attack surface of their systems and software?

Security audit	
Configuration (Correct) management	
Firewall installation	
Data encryption	

Hardening is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including the operating system, web server, application server and applications, etc. In this module, we will introduce configuration management practices that will ensure

systems are installed and maintained according to industry and organizational security standards.

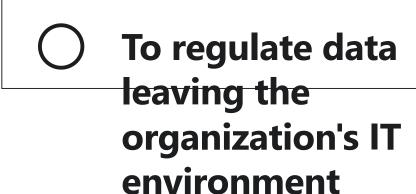
Question 19: Skipped

What is the purpose of data loss prevention (DLP)?

To prevent unauthorized access to the system

To provide entertainment for users

To increase the amount of traffic coming into the infrastructure



(Correct)

# **Explanation**

Egress monitoring is used to regulate data leaving the organization's IT environment. The term currently used in conjunction with this effort is data loss prevention (DLP) or data leak protection.

Question 20: Skipped

What operational problems might an organization encounter with logging facilities?



Increased entertainment for users

Increased speed of the system

Alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded

(Correct)

Operational problems with the logging facility are often related to alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded.

Question 21: Skipped

What is the purpose of configuration management practices?

To ensure systems are

installed and maintained according to industry and organizational security standards

(Correct)

- To ensure systems are installed and maintained according to user preferences To ensure systems are installed and maintained according to manufacturer's recommendations
  - None of the above

In this module, we will introduce configuration management practices that will ensure systems are installed and maintained according to industry and organizational security standards.

Question 22: Skipped What is the lowest level of data sensitivity?			
	Unrestricted public data	(Correct)	
	Moderately res	stricted	
	Highly restricte	ed	
	Low sensitivity		

As this data is already published, no harm can come from further dissemination or disclosure.

Question 23: Skipped

What is the purpose of classifying data?

To ensure it is backed up regularly

To ensure it is treated and

controlled in a manner consistent with the sensitivity of the data

(Correct)





In this section, we will explore the basics of classifying and labeling data to ensure it is treated and controlled in a manner consistent with the sensitivity of the data.

Question 24: Skipped

An organization has classified their data as "low sensitivity". What impact would compromising this data have on the organization?

0	It could lead to loss of temporary competitive advantage
	It could cause minor (Correct) disruptions
	delays or impacts
0	loss of revenue or disruption of planned investments or activities

Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts.

Question 25: Skipped

An organization wants to dispose of some old servers that have confidential data stored on them. What is the most secure method of data destruction? (\*

0	Deleting files	
0	Physical destruction	(Correct)

**Formatting hard drives** 



Destroying the data when it is no longer needed, is the last step in the data life cycle model described in the paragraph. For highly confidential data, physical destruction is the most secure method of data destruction.

Question 26: Skipped

What is the ultimate remedy to data remanence?



Encrypting the device or system



Physical
destruction of
the device or
system

(Correct)

#### **Explanation**

Physical destruction of the device or system is the ultimate remedy to data remanence.

Question 27: Skipped

An organization has created 10 different classifications for data sensitivity. Why is this not typically recommended? (★)

It allows for more precise boundaries between the use of different sensitivity labels It allows for greater ease of data access It could lead to confusion (Correct) among individuals



Typically, two or three classifications are manageable, and more than four tend to be difficult.

Question 28: Skipped

A company handles sensitive customer data and wants to ensure it is treated appropriately. What process can they implement to accomplish this?



Data labeling and classification	(Correct)
Network firewall installation	
Software patch management	

In this section, we will explore the basics of classifying and labeling data to ensure it is treated and controlled in a manner consistent with the sensitivity of the data.

Question 29: Skipped

An organization has a data asset that is no longer useful to them. What should they do with this data?

- Store it in a secure location
  - **Keep it indefinitely**
  - Share it with other organizations

Destroy it in accordance with the policies of the enterprise

and any appropriate legal requirements that may need to be considered

(Correct)

#### **Explanation**

Security professionals should ensure that data destruction is being performed when an asset has reached its retention limit.

Question 30: Skipped

Why is it important to regularly review logs in a computer system?



### incidents and policy violations

- To increase the amount of storage space available
  - To prevent unauthorized access to the system

To provide entertainment for users

#### **Explanation**

Log reviews are an essential function not only for security assessment and testing but also for identifying security

incidents, policy violations, fraudulent activities and operational problems near the time of occurrence.

Question 31: Skipped

An organization applies the longest retention period to all types of information in their records retention policy. Why is this a problem?

It wastes storage

and increases
risk of data
exposure

(Correct)

It reduces the need for periodic reviews of retained records



It is in compliance with all laws and regulations

#### **Explanation**

A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary processing when searching or processing information in search of relevant records.

Question 32: Skipped

An organization is upgrading its computer systems. What should they do to ensure sensitive information is

0	Purge or destroy the old systems (Correct)
0	Leave the old systems as they are
	Donate the old systems to a non-profit organization
0	Encrypt the old systems

not compromised during this process?

**Explanation** 

When system elements are to be removed and replaced, either as part of maintenance upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.

Question 33: Skipped

Which of the following is an example of intellectual property (IP) that should be protected by a DLP solution?

- Financial statementsNetwork configurations
  - Employee personal information

Business plans	(Correct)

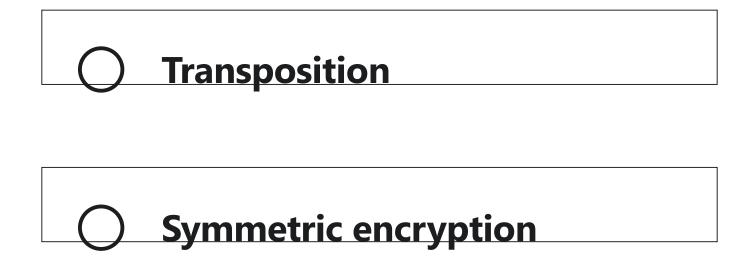
Business plans are an example of intellectual property (IP) that should be protected by a DLP solution, making option a the correct answer.

Question 34: Skipped

Which of the following is NOT a common method of encrypting plaintext? (★)

Asymmetric encryption

Hashing (Correct)



Hashing is not a method of encrypting plaintext, but rather a one-way cryptographic process used to ensure data integrity

Question 35: Skipped

A company is worried about unauthorized access to their data while it is in transit. Which data state is most relevant to this concern?



O In use	
O In motion	(Correct)
At rest	

It also helps put the different data states of in use, at rest and in motion, into context. Data in motion refers to data that is being transmitted over a network or other communication medium.

Question 36: Skipped

Which of the following BEST describes data at rest?

Data processed by an application
Data stored on a (Correct) backup tape
Data being printed from a printer
Data being transmitted over a network

Data at rest refers to data that is not actively being transmitted or processed. It is typically stored in some type of storage medium such as a hard drive, USB drive, or backup tape.

Question 37: Skipped

What is the objective of every encryption system?

To make a message more understandable to unauthorized users

0	To hide or obscure a	
	message so that it cannot be understood by anyone except the intended recipient (Correct)	
	To prevent the	
	transmission of messages	
	To limit the amount of	
	data that can be transmitted	

Γ

Cryptography provides confidentiality by hiding or obscuring a message so that it cannot be understood by anyone except the intended recipient.

Question 38: Skipped

What are some sources from which classifications are derived?

**Employee preferences** 

regulations, contract-specified standards or other business expectations

(Correct)





Classifications are derived from laws, regulations, contractspecified standards or other business expectations.

Question 39: Skipped

What is the purpose of conducting a periodic review of retained records?

To ensure that all information is preserved indefinitely To ensure that information is stored in a secure location To increase the volume of information stored To reduce the volume of information stored and to (Correct) ensure that only

## necessary information is preserved

#### **Explanation**

Organizations should conduct a periodic review of retained records in order to reduce the volume of information stored and to ensure that only necessary information is preserved.

Question 40: Skipped

An organization needs to keep its financial records for seven years, as mandated by law. What type of data retention policy should they implement?



A policy that keeps all data indefinitely A policy that keeps all data for the longest possible period A policy that defines retention (Correct) periods for different types of information

For various types of data, certain industry standards, laws and regulations define retention periods.

Question 41: Skipped

What is data remanence?

Data that is actively being used

Data that might
be left on media (Correct)
after deleting

O Data that is encrypted



Data that might be left on media after deleting is known as remanence and may be a significant security concern.

Question 42: Skipped

How can logs be useful in forensic analysis related to investigations?



They can help make the system run faster They can prevent unauthorized access to the system They can help determine if a vulnerability identified in a (Correct) system has been previously exploited

Review of historic audit logs can determine if a vulnerability identified in a system has been previously exploited.

Question 43: Skipped

What is the difference between ingress monitoring and egress monitoring in terms of data security?

Ingress monitoring and egress monitoring are the same thing

Ingress monitoring refers to surveillance and

assessment of all inbound communications

traffic and access attempts while egress monitoring is used to regulate data leaving the organization's IT environment

(Correct)

Ingress monitoring refers to regulating data leaving the organization's IT environment while egress monitoring is used to assess all inbound communications traffic and access attempts



Ingress monitoring is a security practice that

focuses on monitoring user activity, while egress monitoring focuses on monitoring network traffic.

#### **Explanation**

Ingress monitoring refers to surveillance and assessment of all inbound communications traffic and access attempts while egress monitoring is used to regulate data leaving the organization's IT environment.

Question 44: Skipped

What is the purpose of security labels?

	To store data in a secure location
	To create backups of data
	To encrypt data during transmission
0	To assign a level of sensitivity to (Correct) a data asset

Security labels are part of implementing controls to protect classified information. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires.

Question 45: Skipped

An organization has two sets of data: one that could disrupt some processes if compromised, and one that could lead to the loss of life or threaten the ongoing existence of the organization if compromised. Which set of data is more sensitive?

None of the above

The one that could disrupt some processes if compromised



loss of life or threaten the ongoing existence of the organization if compromised

(Correct)

Both sets of data are equally sensitive

#### **Explanation**

One classification might indicate 'minor, may disrupt some processes' while a more extreme one might be 'grave, could lead to loss of life or threaten ongoing existence of the organization.'

Question 46: Skipped

What is the first step in the change management process?

Request for Change (RFC)	(Correct)
Documentation	
Rollback	
Approval	

The change management process starts with a request for change (RFC) which initiates the process and sets it in motion.

Question 47: Skipped

Why is it important to include social engineering in security awareness training programs?

All of the above (Correct)

It is an inexpensive investment for cyberattackers

It is a basic fieldcraft for espionage agencies



# It can extract significant insider knowledge about organizations or individuals

#### **Explanation**

Social engineering is important to include in security awareness training programs because it is an inexpensive investment for cyberattackers with a potentially high payoff. It can extract significant insider knowledge about organizations or individuals, and many social engineering tactics are not new and have been taught as basic fieldcraft for espionage agencies. People need to be reminded of the threat and types of social engineering so they can recognize and resist a social engineering attack.

Question 48: Skipped

What is a common mistake in records retention?

**Applying the** longest retention period (Correct) to all types of information in an organization **Applying the shortest** retention period to all types of information in an organization

Not having a records retention policy



A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary processing when searching or processing information in search of relevant records.

Question 49: Skipped

Which of the following can be achieved by applying hardening?



Reducing communications attack surface

All of the above (Correct)

Reducing hardware attack surface

#### **Explanation**

Hardening is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including the operating system, web server, application server and applications, etc.

Question 50: Skipped

What is the benefit of having only two or three classifications for data sensitivity?

It allows for more precise boundaries between the use of different sensitivity labels

It allows for greater ease of data access

It allows for manageable

distinctions
between sets of (Correct)
assets with
differing
sensitivity/value



Typically, two or three classifications are manageable, and more than four tend to be difficult.

Question 51: Skipped

What is the first step in any asset management process?

Making an	
inventory	(Correct)

Repairs and maintenance actions **Updating systems and** components **Testing newly installed functionality** 

# **Explanation**

Making an inventory catalog or registry of all the information assets that the organization is aware of is the first step in any asset management process.

Question 52: Skipped

external requirements for data retention are not set?			
	To ignore data retention altogether		
0	To define and implement its own data retention policy (Correct)		
	To keep data for as short a period as possible		
	To keep data for as long as possible		

What is the responsibility of an organization when

When such external requirements are not set, it is an organization's responsibility to define and implement its own data retention policy.

Question 53: Skipped

What is the purpose of a Bring Your Own Device (BYOD) policy? (★)

O Define the appropriate use of an organization's network and computer systems

Specify changes that can be made to a system



Allow workers to acquire

equipment of their choosing and use personally owned equipment for business (and personal) use

(Correct)

#### **Explanation**

The purpose of a BYOD policy is to allow workers to acquire equipment of their choosing and use personally owned equipment for business (and personal) use.

Question 54: Skipped

Why is it important to protect log data from malicious use?

To make the system run faster

To provide entertainment for users

To prevent unauthorized access to the system

The logs contain valuable and

# sensitive information about the organization

(Correct)

#### **Explanation**

Additionally, the logs contain valuable and sensitive information about the organization. Appropriate measures must be taken to protect the log data from malicious use.

Question 55: Skipped

An organization has not defined a data retention policy. What could be the consequences?



0	It could be in violation of	
	externally	
	mandated	(Correct)
	requirements such as	(Correct)
	legislation,	
	regulations or	
	contracts	
0	It could lead to confusion among individuals about how long to keep data	
	It would have no	•

When external requirements are not set, it is an organization's responsibility to define and implement its own data retention policy.

Question 56: Skipped

What is Verification and Audit in Configuration Management?

A process to request changes to a baseline

A process to validate approved changes

(Correct)



A process to ensure all systems have the latest updates

#### **Explanation**

Verification and Audit is a regression and validation process which may involve testing and analysis to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that the currently inuse baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.

Question 57: Skipped

What do classifications of data dictate?

The format in which the data should be stored

Rules and restrictions

about how that information can be used, stored or shared with others

(Correct)

The number of users who can access the data

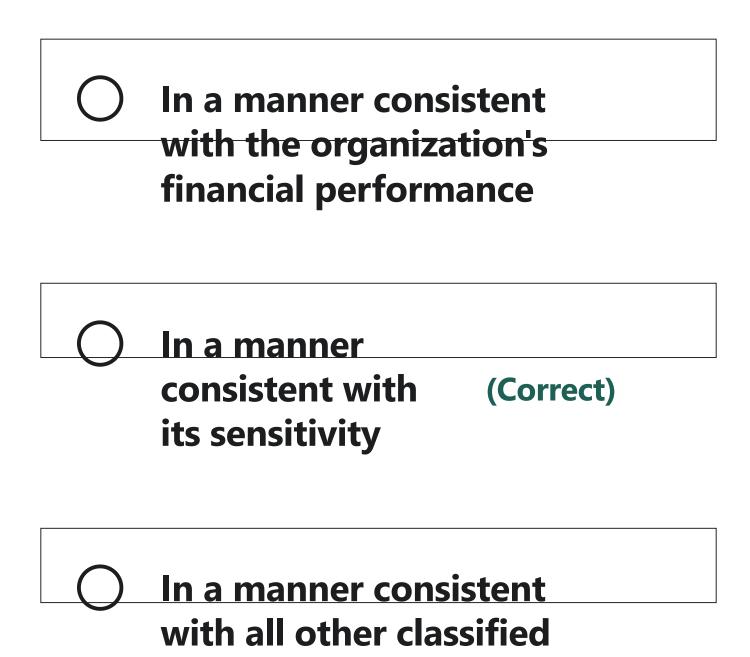


These classifications dictate rules and restrictions about how that information can be used, stored or shared with others.

Question 58: Skipped

A company has classified their data as "minor, may disrupt some processes". How should this data be treated and controlled?





data

These classifications dictate rules and restrictions about how that information can be used, stored or shared with others.

Question 59:	Skipped

What is the main characteristic of symmetric encryption?

- Uses public and private keys
- Uses different keys in encryption and decryption

Uses only one key for encryption

Uses the same key in both

# encryption and decryption

(Correct)

# **Explanation**

The main characteristic of a symmetric algorithm is that it uses the same key in both the encryption and the decryption processes.

Question 60: Skipped

What are the six major sets of activities involved in the data life cycle model?  $(\star)$ 



Creating, modifying, distributing, accessing, archiving, and deleting data

Creating, storing, accessing, sharing, archiving, and deleting data Creating, storing, using, sharing, (Correct) archiving, and destroying data Creating, processing, analyzing, sharing, archiving, and destroying data

All ideas, data, information or knowledge can be thought of as going through six major sets of activities throughout its lifetime. Conceptually, these involve: Creating the knowledge, which is usually tacit knowledge at this point. Storing or recording it in some fashion (which makes it explicit). Using the knowledge, which may cause the information to be modified, supplemented or partially deleted. Sharing the data with other users, whether as a copy or by moving the data from one location to another. Archiving the data when it is temporarily not needed. Destroying the data when it is no longer needed.