

Question 1: **Skipped**

**What is multi-factor authentication?**

☐ **Granting access after demonstrating all three methods of authentication**

☐ **Granting access without demonstrating any methods of authentication**

☐ **Granting access after demonstrating one method of authentication**



**Granting access  
after  
demonstrating  
two or more  
methods of  
authentication**

**(Correct)**

## **Explanation**

MFA is achieved when two of something you are, something you have and something you know is used to authenticate a user.

Question 2: **Skipped**

**What does criticality represent?**



**The importance  
an organization  
gives to data or**

**an information  
system in  
performing its  
operations or  
achieving its  
mission**

**(Correct)**

☐ **All of the above**

☐ **The need for consultation  
with the involved business  
to ensure critical systems  
are identified and  
available**

☐ **The need for security  
professionals to ensure**

**the appropriate levels of availability are provided**

## **Explanation**

Criticality is related to data and systems that are essential for a system to carry out its function

Question 3: **Skipped**

**What is a vulnerability in the context of cybersecurity?**

- ☐ **An inherent weakness or flaw in a system or component that, if triggered or acted upon, could cause a** **(Correct)**

**risk event to  
occur.**

☐ **A measure of the extent to which an entity is protected against potential cyber threats.**

☐ **Something or someone that aims to exploit a vulnerability to thwart protection efforts.**

☐ **A measure of the extent to which an entity is threatened by a potential circumstance or event.**

## **Explanation**

Vulnerability can be any gap that can be exploited to impact the CIA triade of that system

Question 4: **Skipped**

**What is the problem with using knowledge-based authentication alone?**

☐ **It is not vulnerable to any attacks**

☐ **It is not vulnerable to impersonation**

☐ **It is not vulnerable to denial of an action**

☐ **It is often vulnerable to various attacks** **(Correct)**

## **Explanation**

Simply losing the knowledge base information is enough for someone else to authenticate by impersonating as you

Question 5: **Skipped**

**What is the main objective of confidentiality in information security when dealing with sensitive data?**

☐ **Making sure the data is encrypted and decrypted properly**

☐ **Ensuring the data is always accessible when needed**

☐ **All of the above**

☐ **Making sure the data is not disclosed to unauthorized**

**(Correct)**



# individuals or entities

## Explanation

Confidentiality is one of the three key pillars of information security, along with integrity and availability. It refers to the protection of information from unauthorized access, disclosure, or use

Question 6: **Skipped**

**What is the importance of non-repudiation in today's world of e-commerce?**



**It ensures that transactions are conducted offline**

☐ **It ensures that transactions are not conducted online**

☐ **It ensures that people are not held responsible for transactions they did not conduct**

☐ **It ensures that people are held responsible for transactions they conducted** **(Correct)**

# Explanation

In ecommerce non-repudiation ensures that the user cannot deny any transaction he/she carried out

Question 7: **Skipped**

**What does the concept of integrity apply to?**

☐ **Information,  
systems and  
processes for  
business  
operations,  
organizations,  
and people**

**(Correct)**

☐ **Only organizations**

☐ **Only data**

☐ **Only people and their actions**

## **Explanation**

Integrity refers to the adherence to consistency and authenticity. It can apply to information, systems, processes, organizations, and individuals, and is essential for building trust, credibility, and sustainability in various domains.

Question 8: **Skipped**

**What is system integrity?**

☐ **The maintenance of a known bad configuration**

**and unexpected  
operational function as  
the system processes  
information**

- ☐ **The  
maintenance of  
a known good  
configuration  
and expected  
operational  
function as the  
system  
processes  
information** **(Correct)**

- ☐ **The maintenance of a  
random configuration and  
unpredictable operational**

**function as the system  
processes information**

- ☐ **The maintenance of a known configuration and unexpected operational function as the system processes information**

## **Explanation**

This can be a state of the system while it was operating as desired. This can also be state before the system started exhibiting malicious activity.

Question 9: **Skipped**

**What is the term used to describe a type of malware that is capable of self-propagation and can infect multiple systems on a network without the need for human intervention?**

☐ **Virus**

☐ **Worm** **(Correct)**

☐ **Spyware**

☐ **Adware**

## Explanation

Most malware requires user to carry out an activity to spread. Worm explores adjacent assets and propagates without any human intervention

Question 10: **Skipped**

What is the definition of availability in the context of the CIA triad?

☐ **The ability to manipulate data in an unauthorized manner**

☐ **Timely and reliable access to information and the ability to use it for authorized users** (Correct)

☐ **The ability of unauthorized users to access data and information services**





**The guarantee that data and systems are available 100% of the time**

## **Explanation**

Availability ensures that the service is accessible to the relevant individuals for use.

Question 11: **Skipped**

**What is the primary objective of availability in information security?**



**Ensuring data is accurate and unchanged**

☐ **Ensuring data is easily accessible**

☐ **Protecting data from unauthorized access**

☐ **Making sure data is always accessible when needed** **(Correct)**

## **Explanation**

Availability is one of the three core principles of information security, along with confidentiality and integrity. The availability principle ensures that data, systems, and services are available and accessible to authorized users when needed.

Question 12: **Skipped**

**Which of the following is a method of reducing risk by implementing security controls, such as firewalls, intrusion detection systems, and encryption, to prevent cyber attacks and protect against the consequences of a security breach?**

☐ **Risk transfer**

☐ **Risk avoidance**

☐ **Risk mitigation** (Correct)

☐ **Risk acceptance**

# Explanation

Risk mitigation involves taking care of the risk by improving security controls.

Question 13: **Skipped**

**Which of the following security protocols is used to secure communications over the internet and prevent eavesdropping, tampering, and message forgery?**

☐ **FTP**

☐ **SSH** **(Correct)**

☐ **Telnet**

☐ **HTTP**

# Explanation

SSH creates a secure communication method to interact with any system that has been configured

Question 14: **Skipped**

**What does data integrity mean in information security?**

☐ **Making sure data is not lost**

☐ **Protecting data from unauthorized access**

☐ **Ensuring data is accurate and unchanged** **(Correct)**



**Ensuring data can be easily modified**

## Explanation

Data integrity is one of the three core principles of information security, along with confidentiality and availability. The data integrity principle ensures that data is accurate, complete, and unchanged over time. The objective of data integrity is to protect data from unauthorized modification, deletion, or corruption.

Question 15: **Skipped**

What does the term data integrity refer to? (★)



**All of the above** (Correct)

☐ **The assurance that data has not been altered in an unauthorized manner**

☐ **The internal consistency of information**

☐ **The protection of data in systems and during processing**

## **Explanation**

integrity is used extensively in the digital world. This can range from ensuring that the email sent by a user has the original content and has not been tempered with.

Question 16: **Skipped**

**What is the main objective of confidentiality in information security?**

☐ **Ensuring data is easily accessible**

☐ **Protecting data from unauthorized access** **(Correct)**

☐ **Making sure data is not lost**



☐ **Ensuring data can be easily modified**

## **Explanation**

The confidentiality principle ensures that data is protected from unauthorized access and disclosure. The objective of confidentiality is to prevent unauthorized access to sensitive or confidential information, such as personal information, trade secrets, financial data, or intellectual property.

Question 17: **Skipped**

**What is the process of verifying a user's identity called?**

☐ **Authorization**

☐ **Confidentiality**

☐ **Identification**

☐ **Authentication** (Correct)

## Explanation

Authentication is making sure that the user is who he claims to be. This can be done using secret credentials or information unique to that user

Question 18: **Skipped**

**Which of the following security controls is designed to prevent unauthorized access to sensitive information by ensuring that it is only accessible to authorized users?**

☐ **Antivirus**

☐ **Firewall**

☐ **Encryption**

☐ **Access control** **(Correct)**

## Explanation

Access control ensures that information is visible to only relevant people.

Question 19: **Skipped**

**What is sensitivity in the context of confidentiality?**

☐ **The need for protection assigned to information by its owner** (Correct)

☐ **The harm caused to external stakeholders if information is disclosed or modified**

☐ **The ability of information to be accessed only by authorized individuals**



**The health status of an individual**

## **Explanation**

sensitivity can be considered the intensity at which the data needs to be secret. If a document has a confidentiality of top secret , it can only be accessible to people with that clearance

Question 20: **Skipped**

**What is the purpose of creating a baseline in ensuring system integrity?**



**To compare the baseline with the current state of the system**

**(Correct)**

☐ **To protect the information**

☐ **To understand the current state of the system**

☐ **All of the above**

## **Explanation**

Creating a baseline allows to track how much a system has changed or deviated from its original state

Question 21: **Skipped**

**What is the primary advantage of using multi-factor authentication (MFA) over single-factor authentication?**

☐ **MFA is faster and more convenient for users**

☐ **MFA is less secure than single-factor authentication**

☐ **MFA is not commonly used in modern systems**

☐ **MFA provides an additional layer of security by requiring multiple**

**(Correct)**

# methods of authentication

## Explanation

The primary advantage of using multi-factor authentication (MFA) over single-factor authentication is that MFA provides an additional layer of security by requiring multiple methods of authentication.

Question 22: **Skipped**

**What does the term "Availability" in the context of security mean?**

- ☐ **That systems and data are accessible at the time users need them.** **(Correct)**



☐ **That information is protected from unauthorized access**

☐ **That information is recorded, used, and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose**

☐ **That information is only accessible to authorized parties.**

# Explanation

Availability ensures that the service is accessible to the relevant individuals for use.

Question 23: **Skipped**

**What is privacy in the context of information security?**

☐ **Protecting individuals' personal information and ensuring it is not disclosed without their consent.**

**(Correct)**

☐ **Making sure data is always accessible when needed**

☐ **Protecting data from unauthorized access**

☐ **Ensuring data is accurate and unchanged**

## **Explanation**

Privacy is a fundamental right that is protected by many laws and regulations around the world. In the context of information security, privacy refers to protecting personal information from unauthorized access, use, disclosure, or other forms of misuse. Personal information includes any data that can be used to identify an individual, such as name, address, social security number, or medical records

Question 24: **Skipped**

**What is the common best practice for implementing authentication methods?**

☐ **Implementing two of the three common techniques** (Correct)

☐ **Implementing one of the three common techniques**

☐ **Not implementing any of the three common techniques**

☐ **Implementing all three common techniques**

# Explanation

using two factors allow for better security during authentication

Question 25: **Skipped**

**Which of the following is a type of risk that involves the violation of laws, regulations, or industry standards that govern the use and protection of sensitive information and systems?**

☒ **Compliance risk** (Correct)

☐ **Operational risk**

☐ **Information risk**



## Reputational risk

### Explanation

Compliance can vary from industry to industry and compliance risk can cause the organization to violate laws and incur penalty

Question 26: **Skipped**

**What is the purpose of the CIA triad in security?**



**To describe security in a way that only experts can understand**



**To define the purpose of security using irrelevant**

## and meaningless words

☐ **To make security  
more  
understandable to management  
and users** (Correct)

☐ **To create confusion and  
misunderstandings about  
security**

### Explanation

CIA triade is a simplification of all the security concepts. All security controls no matter how complex can be mapped to confidentiality, Integrity and Availability

Question 27: **Skipped**

What is knowledge-based authentication? (★)

☐ **Authentication based on a token or memory card**

☐ **Authentication based on something you do**

☐ **Authentication based on a passphrase or secret code**

**(Correct)**





**Authentication based on  
biometrics or measurable  
characteristics**

## **Explanation**

Knowledge base authentication is something that you know. like a password or passpharese

Question 28: **Skipped**

**What does the security professional need to ensure in  
terms of availability?**



**Data is not accessible to  
authorized users**

☐ **The inaccessibility of data for all users**

☐ **The appropriate levels of availability for critical systems** (Correct)

☐ **The unavailability of critical systems**

## **Explanation**

Availability of a critical system can be essential in smooth functioning of an organization. There can be multiple ways to ensure availability such as redundancy , hot and warm sites etc.

Question 29: **Skipped**

**What is the main challenge in achieving non-repudiation in electronic transactions?**

☐ **Ensuring the authenticity and integrity of the message**

☐ **Ensuring the identity of the sender and recipient is verified**

☐ **Making sure the message is not tampered with during transmission**



**All of the above** (Correct)

## Explanation

Non-repudiation is a security concept that aims to prevent the sender or the recipient of a message from denying having sent or received the message. To achieve non-repudiation in electronic transactions, it is necessary to ensure that the message has not been altered or tampered with during transmission and that the identity of the sender and the recipient is verified. However, ensuring the authenticity and integrity of the message is the main challenge in achieving non-repudiation because electronic messages can be easily intercepted and modified during transmission. Therefore, it is essential to use secure communication channels, such as encrypted connections, digital signatures, and message authentication codes, to ensure that the message remains intact and unaltered throughout the transmission process.

Question 30: **Skipped**

**Which of the following security measures is designed to prevent unauthorized access to a system or network by**

**controlling incoming and outgoing network traffic  
based on predetermined security rules?**

☐ **Antivirus**

☐ **Encryption**

☒ **Firewall** **(Correct)**

☐ **Access control**

## **Explanation**

Firewall monitors and allow the the inbound connections based on certain rules

Question 31: **Skipped**

**What is the term used to describe the likelihood of a particular threat exploiting a vulnerability in an organization's security posture, leading to a security breach or other adverse event?**

☐ **Threat probability** (Correct)

☐ **Threat impact**

☐ **Threat likelihood**

☐ **Threat severity**

# Explanation

Threat probability also known as likelihood of occurrence helps to calculate the severity of a vulnerability. It is the probability of the threat occurring

Question 32: **Skipped**

**What does the term "Confidentiality" in the context of security refer to?**

☐ **Ensuring the completeness, accuracy and internal consistency of information**

☐ **Protecting information from unauthorized access**



**Permitting  
authorized  
access to  
information  
while protecting  
it from improper  
disclosure**

**(Correct)**



**Ensuring systems and data  
are accessible at all times**

## **Explanation**

Part of the CIA triade, confidentiality allows to keep the information visible to only the authorized individual. This could be nay information, such as credit card details or other personally identified information



Question 33: **Skipped**

**Why is the concept of integrity important?**

☐ **It measures the degree to which something is whole and complete**

☒ **All of the above** (Correct)

☐ **It applies to information, systems, processes, organizations, and people**

☐ **It ensures data has not been altered in an**

# unauthorized manner

## Explanation

integrity is used extensively in the digital world. This can range from ensuring that the email sent by a user has the original content and has not been tempered with.

Question 34: **Skipped**

**Which of the following is the first step in the risk management process?**

☐ **Risk assessment**

☐ **Risk  
identification**

**(Correct)**

☐ **Risk response**

☐ **Risk mitigation**

## **Explanation**

Risk identification is used to identify any possible threats and vulnerabilities originating from the chosen functionality and architecture of a system

Question 35: **Skipped**

**What is the definition of "Integrity" in the context of information security?**

☐ **The ability of information to be disclosed only to authorized parties**

- ☐ **The property of information to be recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.** (Correct)

- ☐ **The ability of information to be protected from unauthorized access at all times**

☐ **The ability of information to be made available to users when needed**

## **Explanation**

In security controls, integrity allows a user surety that the information has not been modified and is complete.

Question 36: **Skipped**

**What does internal consistency of information refer to?**

☐ **Data being protected from errors or loss of information**

☐ **Data being displayed and stored the same way on all systems**

☐ **All instances of data being identical in form, content, and meaning** **(Correct)**

☐ **Data being accurate, useful, and complete**

## **Explanation**

All copies of data should be identical to produce useable results. This is ensured using integrity of the copies of the

data

Question 37: **Skipped**

**What is likelihood of occurrence in the context of cybersecurity?**

☐ **The number of vulnerabilities present in a system or network that could be exploited by a threat.**

☐ **The level of difficulty for an attacker to exploit a vulnerability in a system or network.**

- **The probability that a given threat or set of threats will successfully exploit a vulnerability in a system or network, based on a subjective analysis of the threat and attacker capability.**

**(Correct)**



☐ **The measure of the amount of time that a system or network is vulnerable to attack.**

## **Explanation**

likelihood of occurrence helps to calculate the severity of a vulnerability. It is the probability of the threat occurring

Question 38: **Skipped**

**What is the term used to describe a method of securely transmitting data over a network by encapsulating it within another protocol, such as the internet protocol (IP)?**

☐ **Data encryption**

☐ **Tunneling** (Correct)

☐ **Load balancing**

☐ **Network segmentation**

## Explanation

Tunneling creates a private pathway for the data to travel. This could be over public internet and anyone else on the internet won't be able to access the information within that tunnel

Question 39: **Skipped**

What is non-repudiation? (★)

☐ **The protection against an individual falsely denying the occurrence of an action**

☐ **The protection against an individual falsely denying having performed an action** (Correct)

☐ **The protection against an individual falsely accusing someone else of performing an action**

- ☐ **The protection against an individual falsely admitting having performed an action**

## **Explanation**

non-reduciation is used for auditing purpose and tracks the activity a user carries out and ensure that activity is tamper proof thus maintaining its integrity

Question 40: **Skipped**

**What is a threat in the context of cybersecurity?**

- ☐ **An inherent weakness or flaw in a system or component.**

☐ **The means by which a threat actor carries out their objectives.**

☐ **Something in need of protection.**

☐ **A person or thing that takes action to exploit a target organization's system vulnerabilities.**

**(Correct)**

# Explanation

Threat is the possibility of q exploiting a vulnerability. This could be done by anyone such as a human, an automated script or a state actor

Question 41: **Skipped**

**What is the purpose of non-repudiation in information security?**

☐ **To prevent the sender or recipient of a message from denying having sent or received the message**

**(Correct)**

☐ **To ensure data is always accessible when needed**

☐ **To protect data from unauthorized access**

☐ **To ensure data is accurate and unchanged**

## **Explanation**

Non-repudiation is a security service that ensures that the sender and recipient of a message cannot deny having sent or received the message. This is typically achieved through the use of digital signatures or other cryptographic techniques that provide proof of the message's origin, integrity, and receipt.

Question 42: **Skipped**

**What is the primary factor in the reliability of information and systems?**

☒ **Integrity** (Correct)

☐ **Confidentiality**

☐ **Availability**

☐ **Authenticity**

## Explanation

For a data to be reliable and produce useful results the integrity of that data should be ensured

Question 43: **Skipped**



Which of the following is a method of protecting against unauthorized access to a system or network by requiring users to provide two or more authentication factors?

☐ **Two-factor authentication** (Correct)

☐ **Token-based authentication**

☐ **Single sign-on**

☐ **Federated authentication**

# Explanation

Two factor authentication utilizes information such as something you have apart from the traditional something you are

Question 44: **Skipped**

**What does the CIA triad refer to?**

☐ **Confidentiality, Identity,  
and Authentication**

☐ **Confidentiality,  
Integrity, and  
Availability** **(Correct)**

☐ **Confidentiality,  
Intelligence, and  
Authenticity**

☐ **Confidentiality,  
Intelligence, and  
Authorization**

## **Explanation**

CIA triade is a simplification of all the security concepts. All security controls no matter how complex can be mapped to confidentiality, Integrity and Availability

Question 45: **Skipped**

**What is an asset in the context of cybersecurity?**

☐ **A person or thing that takes action to exploit a target organization's system vulnerabilities.**

☐ **A gap or weakness in protection efforts.**

☐ **Something in need of protection.** **(Correct)**

☐ **The means by which a threat actor carries out their objectives.**

# Explanation

Asset can be anything tangible such as a computer or a server or intangible like a database

Question 46: **Skipped**

**Why is integrity a primary factor in the reliability of information and systems?**

☐ **Because the need to compromise information and system integrity may be dictated by laws and regulations or the needs of the organization to access and use unreliable, inaccurate information**

☐ **Because the need to**

**safeguard  
information and  
system integrity  
may be dictated  
by laws and  
regulations or  
the needs of the  
organization to  
access and use  
reliable,  
accurate  
information**

**(Correct)**

- ☐ **Because the need to  
ignore information and  
system integrity may be  
dictated by laws and  
regulations or the needs  
of the organization to**

**access and use reliable,  
accurate information.**

- ☐ **Because the need to ignore information and system integrity may be dictated by laws and regulations or the needs of the organization to access and use unreliable, inaccurate information**

## **Explanation**

Any data processed on a system that has not maintained its integrity is questionable and is of no use. Thus ensuring the integrity of a system is essential.

Question 47: **Skipped**

What is single-factor authentication?

☐ **Granting access after demonstrating one method of authentication** (Correct)

☐ **Granting access without demonstrating any methods of authentication**

☐ **Granting access after demonstrating all three methods of authentication**





**Granting access after demonstrating two or more methods of authentication**

## **Explanation**

This could be something simple as username and password for a social media account and punch code for attendance system

Question 48: **Skipped**

**What does Personally Identifiable Information (PII) pertain to?**

☐ **Data about an individual that could be used to identify them** (Correct)

☐ **The importance assigned to information by its owner**

☐ **Information about an individual's health status**

☐ **Trade secrets, research, business plans and intellectual property**

# Explanation

PII is a set of sensitive information that can help identify the user from who the information is collected. This can be name , address and credit card number. Information such as gender are not considered PII

Question 49: **Skipped**

**What is the most important aspect of privacy in the context of information security?**

☐ **All of the above**

☐ **Protecting  
personal  
information  
from  
unauthorized  
access or  
disclosure**

**(Correct)**

☐ **Making sure data is always accessible when needed**

☐ **Ensuring data is accurate and unchanged**

## **Explanation**

Privacy is a critical concern in information security, especially in today's digital age, where personal information is being collected and stored on an unprecedented scale. Protecting personal information is essential to ensure that individuals can trust organizations to handle their information responsibly and prevent the risk of identity theft, fraud, or other forms of malicious activity.

Question 50: **Skipped**

What is the definition of a threat vector in the context of cybersecurity? (★)

☐ **A measure of the extent to which an entity is threatened by a potential circumstance or event.**

☐ **An inherent weakness or flaw in a system or component.**

☐ **A person or thing that takes action to exploit a target organization's system vulnerabilities.**

☐ **The means by which a threat**

**(Correct)**

**actor carries out  
their objectives.**

## **Explanation**

The method used to exploit a vulnerability is called the threat vector

Question 51: **Skipped**

**What is multi-factor authentication (MFA)?**



**A type of  
authentication  
that uses two or  
more methods**

**(Correct)**

☐ **A type of authentication  
that uses only one method**

☐ **A type of authentication  
that uses only one factor**

☐ **A type of authentication  
that uses only two  
methods**

## **Explanation**

Multi-factor authentication (MFA) is a type of authentication that uses more than two methods to verify the identity of a user. MFA is a security mechanism that requires users to provide multiple forms of authentication in order to access a system or service. Typically, MFA requires users to provide something they know (such as a password or PIN), something they have (such as a smart card or token),

and/or something they are (such as a biometric identifier like a fingerprint or face scan).

Question 52: **Skipped**

**What is data integrity?**

☐ **The assurance that data has been altered in a proper manner**

☐ **The assurance that data has been altered in an unauthorized manner**

☐ **The assurance that data has been altered in a authorized manner**





**The assurance  
that data has  
not been altered  
in any manner**

**(Correct)**

## **Explanation**

Integrity is used extensively in the digital world. This can range from ensuring that the email sent by a user has the original content and has not been tempered with.

Question 53: **Skipped**

**What is the purpose of the CIA triad terms?**



**To define the purpose of  
security**

☐ **To describe security using relevant and meaningful words**

☒ **All of the above** (Correct)

☐ **To make security more understandable to management and users**

## **Explanation**

CIA triade is a simplification of all the security concepts. All security controls no matter how complex can be mapped to confidentiality, Integrity and Availability

Question 54: **Skipped**

**What is the term used to describe an unauthorized or illegal act that is performed using a computer or network, such as hacking, phishing, or malware distribution?**

☐ **Information technology**

☐ **Cybersecurity**

☐ **Cybercrime** **(Correct)**

☐ **Data protection**

# Explanation

Cybercrime involves activity to impact the CIA triade of an organization.

Question 55: **Skipped**

**What are the three common methods of authentication?**

☐ **Something you know,  
something you have, something you are** (Correct)

☐ **Something you have,  
something you do,  
somewhere you are**

☐ **Something you do,  
something you trust,  
something you have**

☐ **Something you have,  
someone you know,  
something you do**

## **Explanation**

All these are different types of data and allow for depth in authentication. As not all can be compromised in a single time and using multi factors allow for more security with authentication

Question 56: **Skipped**

**What is the term used to describe the process of removing or neutralizing malicious software (malware) from a computer**

☐ **Firewall configuration**

☐ **Decryption**

☐ **Malware removal** **(Correct)**

☐ **Encryption**

## **Explanation**

This is the process to quarantine the malware and stop the damage caused by it.

Question 57: **Skipped**

Which of the following is a systematic approach to protecting against cyber threats that involves a continuous cycle of identifying, assessing, and prioritizing risks and implementing measures to reduce or eliminate those risks?

☐ **Security assessment**

☐ **Incident response**

☐ **Risk management** (Correct)

☐ **Penetration testing**

# Explanation

Risk management involves taking action based on the criticality of the risk.

Question 58: **Skipped**

**Which of the following is a type of risk that involves the unauthorized use or disclosure of confidential information, such as passwords, financial data, or personal information?**

☐ **Information risk** (Correct)

☐ **Operational risk**

☐ **Reputational risk**





**Compliance risk**

## Explanation

Information risk involves weak access control and areas that can leak sensitive information

Question 59: **Skipped**

What is the term used to describe the practice of dividing a network into smaller, isolated segments to reduce the risk of cyber-attacks? (★)



**Network  
segmentation**

**(Correct)**



**Router configuration**

☐ **Virtual private network**

☐ **Load balancing**

## **Explanation**

Network segmentation allows to create logical segment that are isolated and information does not travel between those segments unless configured to do so.

Question 60: **Skipped**

**What does the term sensitivity refer to?**

☐ **The harm to external stakeholders from improper disclosure or**

## **modification of information**

- ☐ **The importance assigned to information by its owner or the purpose of denoting its need for protection** (Correct)

- ☐ **The value of information to an organization or individual**



# The confidentiality of information

## Explanation

sensitivity can be considered the intensity at which the data needs to be secret. If a document has a confidentiality of top secret , it can only be accessible to people with that clearance