



BCS CISMP-V9 Practice Questions

Shared by Jefferson on 12-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

When considering outsourcing the processing of data, which two legal "duty of care" considerations SHOULD the original data owner make?

- 1 Third party is competent to process the data securely.
2. Observes the same high standards as data owner.
3. Processes the data wherever the data can be transferred.
4. Archive the data for long term third party's own usage.

Options:

- A- 2 and 3.
- B- 3 and 4.
- C- 1 and 4.
- D- 1 and 2.

Answer:

D

Explanation:

When outsourcing data processing, the original data owner has a legal duty of care to ensure that the third party is competent to process the data securely (1) and observes the same high standards as the data owner (2). This means that the third party must have the necessary skills, knowledge, and security measures in place to protect the data, and they must adhere to the same level of data protection and privacy standards as the original owner. Processing the data wherever it can be transferred (3) and archiving the data for the third party's own long-term usage (4) are not primary legal considerations and may, in fact, contravene data protection laws if done without proper safeguards and compliance with regulations.

Question 2

Question Type: MultipleChoice

What does a penetration test do that a Vulnerability Scan does NOT?

Options:

- A- A penetration test seeks to actively exploit any known or discovered vulnerabilities.
- B- A penetration test looks for known vulnerabilities and reports them without further action.
- C- A penetration test is always an automated process - a vulnerability scan never is.
- D- A penetration test never uses common tools such as Nmap, Nessus and Metasploit.

Answer:

A

Explanation:

A penetration test, unlike a vulnerability scan, is an in-depth process where security professionals actively attempt to exploit vulnerabilities in a system. The goal is to simulate a real-world attack to understand how an attacker could exploit vulnerabilities and to determine the potential impact. This involves not just identifying vulnerabilities, as a scan does, but also attempting to exploit them to understand the full extent of the risk. Penetration tests are typically manual or semi-automated and involve a variety of tools and techniques to uncover and exploit security weaknesses, which can include common tools like Nmap, Nessus, and Metasploit.

Question 3

Question Type: MultipleChoice

Which option best is MOST LIKELY to be described as a consequential loss?

Options:

- A- Reputation damage.
- B- Monetary theft.
- C- Service disruption.
- D- Processing errors.

Answer:

A

Explanation:

Consequential loss in the context of information security refers to secondary or indirect damage that occurs as a result of a primary event or incident. It is not the immediate direct loss, such as theft of money or service disruption, but rather the subsequent impact that may not be immediately apparent. Reputation damage is a prime example of consequential loss because it is a secondary effect that can occur after a security breach or incident. The loss of trust by customers, partners, and stakeholders can have long-term negative effects on a business's financial health and market position. This type of loss is often more significant and lasting than the immediate direct costs associated with an incident.

Question 4

Question Type: MultipleChoice

Which of the following is NOT an information security specific vulnerability?

Options:

- A- Use of HTTP based Apache web server.
- B- Unpatched Windows operating system.
- C- Confidential data stored in a fire safe.
- D- Use of an unlocked filing cabinet.

Answer:

C

Explanation:

In the context of information security vulnerabilities, we are typically referring to weaknesses that can be exploited by threats to compromise the confidentiality, integrity, or availability of an information system. Options A, B, and D all represent potential vulnerabilities:

A: Use of HTTP for an Apache web server could allow for interception of data due to lack of encryption.

B: An unpatched Windows operating system could have known security flaws that can be exploited.

D: An unlocked filing cabinet could lead to unauthorized physical access to sensitive documents.

Option C, however, refers to the storage of confidential data in a fire safe, which is a protective measure rather than a vulnerability. A fire safe is designed to protect physical assets from damage or destruction, particularly in the event of a fire, and does not inherently contain a weakness that could be exploited by a cyber threat. Therefore, it is not considered an information security specific vulnerability.

Question 5

Question Type: MultipleChoice

Which of the following acronyms covers the real-time analysis of security alerts generated by applications and network hardware?

Options:

- A- CERT
- B- SIEM.
- C- CISM.
- D- DDoS.

Answer:

B

Explanation:

SIEM, which stands for Security Information and Event Management, is the correct acronym that covers the real-time analysis of security alerts generated by applications and network hardware. SIEM systems aggregate and analyze activity data from various resources across the IT infrastructure, such as network devices, servers, and domain controllers. They operate on rules-based and statistical correlation algorithms to establish relationships between log entries, providing reports on security-related incidents and events, and sending alerts if the analysis indicates a potential security issue. This enables organizations to gain insights into their security posture, identify trends, and detect threats or anomalies that could indicate a security incident.

Question 6

Question Type: MultipleChoice

Which standards framework offers a set of IT Service Management best practices to assist organisations in aligning IT service delivery with business goals - including security goals?

Options:

- A- ITIL.
- B- SABSA.
- C- COBIT
- D- ISAGA.

Answer:

A

Explanation:

ITIL (Information Technology Infrastructure Library) is a widely recognized framework that offers a comprehensive set of best practices for IT Service Management (ITSM). It assists organizations in aligning IT services with business goals, including security objectives. ITIL provides guidance on the entire service lifecycle, from service strategy and design to service transition, operation, and continual service improvement. By following ITIL's structured approach, organizations can enhance the quality of IT services, manage risk effectively, improve customer satisfaction, and ensure that IT and business strategies are in sync.

Question 7

Question Type: MultipleChoice

When undertaking disaster recovery planning, which of the following would NEVER be considered a "natural" disaster?

Options:

- A- Arson.
- B- Electromagnetic pulse
- C- Tsunami.
- D- Lightning Strike

Answer:

A

Explanation:

Arson is an act of intentionally setting fire to property for malicious reasons. It is a criminal act and is not classified as a natural disaster. Natural disasters are events that occur due to natural processes of the Earth, such as tsunamis, lightning strikes, and other weather-related events. An electromagnetic pulse can be a natural event if it is caused by solar flares or a man-made event if it is the result of a nuclear explosion. However, arson is always the result of human activity and is not caused by natural processes¹.

P2P
exams

Question 8

Question Type: MultipleChoice

By what means SHOULD a cloud service provider prevent one client accessing data belonging to another in a shared server environment?

Options:

- A- By ensuring appropriate data isolation and logical storage segregation.
- B- By using a hypervisor in all shared servers.
- C- By increasing deterrent controls through warning messages.
- D- By employing intrusion detection systems in a VMs.

P2P
exams

Answer:

A

Explanation:

In a shared server environment, such as cloud services, it's crucial to maintain the confidentiality and integrity of client data. The most effective way to prevent one client from accessing another's data is through data isolation and logical storage segregation. This approach aligns with the Information Security Management Principles, specifically under the domain of Technical Security Controls. Data isolation ensures that each client's data is processed and stored separately, while logical storage segregation uses software controls to keep data separate even when stored on the same physical server. This method is part of a broader set of security controls that include encryption, access controls, and regular audits to

ensure compliance with security policies.

Question 9

Question Type: MultipleChoice

How does network visualisation assist in managing information security?

Options:

- A- Visualisation can communicate large amounts of data in a manner that is a relatively simple way for people to analyse and interpret.
- B- Visualisation provides structured tables and lists that can be analysed using common tools such as MS Excel.
- C- Visualisation offers unstructured data that records the entirety of the data in a flat, filterable file format.
- D- Visualisation software operates in a way that is rarely and thereby it is less prone to malware infection.

Answer:

A

Explanation:

Network visualization is a powerful tool in managing information security as it can transform complex data sets into visual formats that are easier to understand and analyze. This is particularly useful in cybersecurity, where large volumes of data need to be monitored for potential security threats. Effective data visualization can provide meaningful insights into network security data, helping analysts to quickly identify patterns, anomalies, and trends that may indicate security incidents¹².

While options B and C are methods of data analysis, they do not leverage the unique capabilities of visualization for rapid interpretation of security data. Option D is incorrect because the operation of visualization software does not inherently reduce malware infection risks; it's the insights gained from visualization that can assist in proactive threat detection and management¹².

Effective Data Visualization in Cybersecurity, IEEE Conference¹.

A Survey of Visualization Systems for Network Security, IEEE Transactions².

Question 10

Question Type: MultipleChoice

Which of the following describes a qualitative risk assessment approach?

Options:

- A- A subjective assessment of risk occurrence likelihood against the potential impact that determines the overall severity of a risk.
- B- The use of verifiable data to predict the risk occurrence likelihood and the potential impact so as to determine the overall severity of a risk.
- C- The use of Monte-Carlo Analysis and Layers of Protection Analysis (LOPA) to determine the overall severity of a risk.
- D- The use of Risk Tolerance and Risk Appetite values to determine the overall severity of a risk

Answer:

A

Explanation:

A qualitative risk assessment approach is characterized by the subjective analysis of the likelihood of a risk occurring and its potential impact. This method relies on the judgment and experience of the assessor to estimate the severity of a risk. It does not use numerical data or statistical methods, which are typical of quantitative assessments. Instead, it may use descriptors like 'low', 'medium', or 'high' to rate both the likelihood of occurrence and the potential impact. This approach is useful when precise data is unavailable or when assessing complex, multifaceted risks where human insight is valuable.

To Get Premium Files for CISMP-V9 Visit

<https://www.p2pexams.com/products/cismp-v9>

For More Free Questions Visit

<https://www.p2pexams.com/bcs/pdf/cismp-v9>

20%
DISCOUNT

P2P
exams