ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: BCS

Code: CISMP-V9

Exam: BCS Foundation Certificate in Information Security Management Principles V9.0

https://www.examsnest.com/exam/cismp-v9/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.1

Question: 1

Which of the following is NOT an accepted classification of security controls?

A. Nominative.
B. Preventive.
C. Detective.
D. Corrective.

Answer: A

Explanation:

Security controls are measures taken to safeguard an information system from attacks or to mitigate the impact of a breach. They are commonly classified into three main categories: preventive, detective, and corrective. Preventive controls aim to prevent incidents before they occur, detective controls are designed to discover and detect security events, and corrective controls are intended to restore systems to normal operation after an incident. The term “nominative” is not recognized as a standard classification of security controls within the principles of information security management. Instead, the accepted classifications align with the objectives of protecting the confidentiality, integrity, and availability of information. Reference: The BCS Foundation Certificate in Information Security Management Principles outlines the categorization, operation, and effectiveness of controls of different types and characteristics, which does not include “nominative” as a classification1.

Question: 2

Which three of the following characteristics form the AAA Triad in Information Security?
1. Authentication
2. Availability
3. Accounting
4. Asymmetry
5. Authorisation

A. 1, 2 and 3.
B. 2, 4, and 5.
C. 1, 3 and 4.
D. 1, 3 and 5.

Answer: D

Explanation:

The AAA Triad in Information Security stands for Authentication, Authorization (also known as Authorisation), and Accounting. These three components are fundamental to ensuring that access to systems is controlled and monitored:
Authentication is the process of verifying the identity of a user or entity. It ensures that individuals are who they claim to be. This can involve methods such as passwords, biometrics, or tokens.
Authorization determines what an authenticated user is allowed to do. It involves granting or denying rights to access resources and perform actions within a system based on the user's identity.
Accounting keeps track of user activities. This includes logging when users log in and out, what actions they perform, and what resources they access. It's essential for auditing purposes and can also be used for billing or analyzing resource usage.
These principles are designed to protect information by managing potential risks and controlling access to data. They are part of a broader framework that includes physical, technical, and procedural controls to safeguard information assets.
Reference := The explanation provided is based on standard definitions and practices within the field of Information Security Management, as outlined in resources like the BCS Foundation Certificate in Information Security Management Principles and corroborated by industry sources1234.

Question: 3

According to ISO/IEC 27000, which of the following is the definition of a vulnerability?

A. A weakness of an asset or group of assets that can be exploited by one or more threats.
B. The impact of a cyber attack on an asset or group of assets.
C. The threat that an asset or group of assets may be damaged by an exploit.
D. The damage that has been caused by a weakness iin a system.

Answer: A

Explanation:

The term 'vulnerability' within the context of ISO/IEC 27000 refers to any weakness present in an asset or group of assets that could potentially be exploited by one or more threats. This definition aligns with the concept of vulnerability as a gap in protection efforts that, if not addressed, could allow a threat to compromise the confidentiality, integrity, or availability of an asset. It is important to note that vulnerabilities can be identified in various components of an organization's infrastructure, including hardware, software, processes, and even personnel. Effective information security management involves identifying these vulnerabilities through risk assessments and implementing appropriate controls to mitigate the risk of exploitation.
Reference: The definition provided aligns with the information found in ISO/IEC 27000:2018, which provides an overview of information security management systems (ISMS) and includes terms and definitions commonly used in the ISMS family of standards12.

Question: 4

Which term describes the acknowledgement and acceptance of ownership of actions, decisions, policies and deliverables?

A. Accountability.
B. Responsibility.
C. Credibility.
D. Confidentiality.

Answer: A

Explanation:

Accountability is the term that describes the acknowledgement and acceptance of ownership of actions, decisions, policies, and deliverables. It implies that an individual or organization is willing to take responsibility for their actions and the outcomes of those actions, and is answerable to the relevant stakeholders. This concept is fundamental in information security management, as it ensures that individuals and teams are aware of their roles and the expectations placed upon them, particularly in relation to the protection of information assets. Accountability cannot be delegated; while tasks can be assigned to others, the ultimate ownership and obligation to report and justify the outcomes remain with the accountable party.
Reference: = The BCS Foundation Certificate in Information Security Management Principles outlines the importance of accountability within the context of information security management. It is a key principle that supports the governance of information security and the management of risks associated with information assets1.

Question: 5

Which security concept provides redundancy in the event a security control failure or the exploitation of a vulnerability?

A. System Integrity.
B. Sandboxing.
C. Intrusion Prevention System.
D. Defence in depth.

Answer: D

Explanation:

Defence in depth is a security concept that involves implementing multiple layers of security controls throughout an information system. The idea is that if one control fails or a vulnerability is exploited, other controls will provide redundancy and continue to protect the system. This approach is analogous to a physical fortress with multiple walls; if an attacker breaches one wall, additional barriers exist to stop them from progressing further. In the context of information security, this could include a combination of firewalls, intrusion detection systems, antivirus software, and strict access controls, among others. Defence in depth is designed to address security vulnerabilities not only in technology but also in processes and people, acknowledging that human error or negligence can often lead to security breaches.
Reference: The concept of defence in depth aligns with the Information Security Management Principles as outlined by BCS, particularly under the domains of Technical Security Controls and Disaster Recovery and Business Continuity Management. It is also supported by various industry sources that describe defence in depth as a strategy that leverages multiple security measures to

protect an organization's assets12345.

Online retailers are the most at risk for the theft of electronic-based credit card data due to the nature of their business, which involves processing a large volume of transactions over the internet. This exposes them to various cyber threats, including hacking, phishing, and other forms of cyber-attacks that can compromise credit card information. Traditional market traders, mail delivery businesses, and agricultural producers typically do not handle credit card transactions to the same extent or in the same electronic manner as online retailers, making them less likely targets for this specific type of data theft.

The principles of Information Security Management emphasize the importance of protecting sensitive data, such as credit card information, through technical security controls and risk management practices. Online retailers must implement robust security measures, including encryption, secure payment gateways, and regular security audits, to mitigate the risks associated with electronic transactions12.

Reference :=

BCS Information Security Management Principles, particularly the sections on Technical Security Controls and Information Risk, provide guidance on protecting electronic data and managing the associated risks1.

Additional insights can be found in the Information Security Management Principles, 3rd Edition by Andy Taylor, David Alexander, Amanda Finch, David Sutton2.

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: BCS

Code: CISMP-V9

Exam: BCS Foundation Certificate in Information Security Management Principles V9.0

https://www.examsnest.com/exam/cismp-v9/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation