



BCS

Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0

NEW QUESTION 1

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

NEW QUESTION 2

For which security-related reason SHOULD staff monitoring critical CCTV systems be rotated regularly during each work session?

- A. To reduce the chance of collusion between security staff and those being monitored.
- B. To give experience to monitoring staff across a range of activities for training purposes.
- C. Health and Safety regulations demand that staff are rotated to prevent posture and vision related harm.
- D. The human attention span during intense monitoring sessions is about 20 minutes.

Answer: D

NEW QUESTION 3

What form of training SHOULD developers be undertaking to understand the security of the code they havewritten and how it can improvesecurity defence whilst being attacked?

- A. Red Team Training.
- B. Blue Team Training.
- C. Black Hat Training.
- D. Awareness Training.

Answer: C

NEW QUESTION 4

What physical security control would be used to broadcast false emanations to mask the presence of true electromagnetic emanations fromgenuine computing equipment?

- A. Faraday cage.
- B. Unshielded cabling.
- C. Copper infused windows.
- D. White noise generation.

Answer: B

NEW QUESTION 5

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

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

Answer: B

Explanation:

https://en.wikipedia.org/wiki/Security_information_and_event_management

NEW QUESTION 6

Why is it prudent for Third Parties to be contracted to meet specific security standards?

- A. Vulnerabilities in Third Party networks can be malevolently leveraged to gain illicit access into client environments.
- B. It is a legal requirement for Third Party support companies to meet client security standards.
- C. All access to corporate systems must be controlled via a single set of rules if they are to be enforceable.
- D. Third Parties cannot connect to other sites and networks without a contract of similar legal agreement.

Answer: C

NEW QUESTION 7

Which cryptographic protocol preceded Transport Layer Security (TLS)?

- A. Public Key Infrastructure (PKI).

- B. Simple Network Management Protocol (SNMP).
- C. Secure Sockets Layer (SSL).
- D. Hypertext Transfer Protocol Secure (HTTPS)

Answer: C

NEW QUESTION 8

What Is the PRIMARY security concern associated with the practice known as Bring Your Own Device (BYOD) that might affect a large organisation?

- A. Most BYOD involves the use of non-Windows hardware which is intrinsically insecure and open to abuse.
- B. The organisation has significantly less control over the device than over a corporately provided and managed device.
- C. Privately owned end user devices are not provided with the same volume nor frequency of security patch updates as a corporation.
- D. Under GDPR it is illegal for an individual to use a personal device when handling personal information under corporate control.

Answer: A

NEW QUESTION 9

Which security framework impacts on organisations that accept credit cards, process credit card transactions, store relevant data or transmit credit card data?

- A. PCI DSS.
- B. TOGAF.
- C. ENISA NIS.
- D. Sarbanes-Oxley

Answer: A

Explanation:

<https://digitalguardian.com/blog/what-pci-compliance>

NEW QUESTION 10

What aspect of an employee's contract of employment is designed to prevent the unauthorised release of confidential data to third parties even after an employee has left their employment?

- A. Segregation of Duties.
- B. Non-disclosure.
- C. Acceptable use policy.
- D. Security clearance.

Answer: B

NEW QUESTION 10

Which types of organisations are likely to be the target of DDoS attacks?

- A. Cloud service providers.
- B. Any financial sector organisations.
- C. Online retail based organisations.
- D. Any organisation with an online presence.

Answer: D

NEW QUESTION 13

Which of the following describes a qualitative risk assessment approach?

- 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: C

NEW QUESTION 18

In a security governance framework, which of the following publications would be at the HIGHEST level?

- A. Procedures.
- B. Standards
- C. Policy.
- D. Guidelines

Answer: A

NEW QUESTION 21

What is the root cause as to why SMS messages are open to attackers and abuse?

- A. The store and forward nature of SMS means it is considered a 'fire and forget service'.
- B. SMS technology was never intended to be used to transmit high risk content such as One-time payment codes.

- C. The vast majority of mobile phones globally support the SMS protocol inexpensively.
- D. There are only two mobile phone platforms - Android and iOS - reducing the number of target environments.

Answer: B

NEW QUESTION 23

What term is used to describe the testing of a continuity plan through a written scenario being used as the basis for discussion and simulation?

- A. End-to-end testing.
- B. Non-dynamic modeling
- C. Desk-top exercise.
- D. Fault stressing
- E. C

Answer: E

NEW QUESTION 24

When an organisation decides to operate on the public cloud, what does it lose?

- A. The right to audit and monitor access to its information.
- B. Control over Intellectual Property Rights relating to its applications.
- C. Physical access to the servers hosting its information.
- D. The ability to determine in which geographies the information is stored.

Answer: A

NEW QUESTION 25

Which of the following cloud delivery models is NOT intrinsically "trusted" in terms of security by clients using the service?

- A. Public.
- B. Private.
- C. Hybrid.
- D. Community

Answer: D

NEW QUESTION 26

Which type of facility is enabled by a contract with an alternative data processing facility which will provide HVAC, power and communications infrastructure as well as computing hardware and a duplication of organisations existing "live" data?

- A. Cold site.
- B. Warm site.
- C. Hot site.
- D. Spare site

Answer: A

NEW QUESTION 28

You are undertaking a qualitative risk assessment of a likely security threat to an information system. What is the MAIN issue with this type of risk assessment?

- A. These risk assessments are largely subjective and require agreement on rankings beforehand.
- B. Dealing with statistical and other numeric data can often be hard to interpret.
- C. There needs to be a large amount of previous data to "train" a qualitative risk methodology.
- D. It requires the use of complex software tools to undertake this risk assessment.

Answer: D

NEW QUESTION 32

Which algorithm is a current specification for the encryption of electronic data established by NIST?

- A. RSA.
- B. AES.
- C. DES.
- D. PGP.

Answer: B

Explanation:

<https://www.nist.gov/publications/advanced-encryption-standard-aes>

NEW QUESTION 37

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?

- A. ITIL.

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

Answer: A

Explanation:

<https://www.cherwell.com/it-service-management/library/essential-guides/essential-guide-to-iti-framework-and>

NEW QUESTION 40

Why should a loading bay NEVER be used as a staff entrance?

- A. Loading bays are intrinsically vulnerable, so minimising the people traffic makes securing the areas easier and more effective.
- B. Loading bays are often dirty places, and staff could find their clothing damaged or made less appropriate for the office.
- C. Most countries have specific legislation covering loading bays and breaching this could impact on insurance status.
- D. Staff should always enter a facility via a dedicated entrance to ensure smooth access and egress.

Answer: D

NEW QUESTION 42

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CISMP-V9 Practice Exam Features:

- * CISMP-V9 Questions and Answers Updated Frequently
- * CISMP-V9 Practice Questions Verified by Expert Senior Certified Staff
- * CISMP-V9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISMP-V9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CISMP-V9 Practice Test Here](#)