

BCS

Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0



NEW QUESTION 1

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 2

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 3

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 4

What type of attack could directly affect the confidentiality of an unencrypted VoIP network?

- A. Packet Sniffing.
- B. Brute Force Attack.
- C. Ransomware.
- D. Vishing Attack

Answer: B

NEW QUESTION 5

What term is used to describe the act of checking out a privileged account password in a manner that bypasses normal access controls/procedures during a critical emergency situation?

- A. Privileged User Gateway
- B. Enterprise Security Management
- C. Multi Factor Authentication.
- D. Break Glass

Answer: C

NEW QUESTION 6

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 7

What form of risk assessment is MOST LIKELY to provide objective support for a security Return on Investment case?

- A. ISO/IEC 27001.
- B. Qualitative.
- C. CPNI.
- D. Quantitative

Answer: D

NEW QUESTION 8

In terms of security culture, what needs to be carried out as an integral part of security by all members of an organisation and is an essential component to any security regime?

- A. The 'need to know' principle.
- B. Verification of visitor's ID
- C. Appropriate behaviours.
- D. Access denial measures

Answer: D

NEW QUESTION 9

When calculating the risk associated with a vulnerability being exploited, how is this risk calculated?

- A. Risk = Likelihood * Impact.
- B. Risk = Likelihood / Impact.
- C. Risk = Vulnerability / Threat.
- D. Risk = Threat * Likelihood.

Answer: C

NEW QUESTION 10

Which of the following types of organisation could be considered the MOST at risk from the theft of electronic based credit card data?

- A. Online retailer.
- B. Traditional market trader.
- C. Mail delivery business.
- D. Agricultural producer.

Answer: A

NEW QUESTION 10

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.

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

Answer: C

NEW QUESTION 11

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 13

What form of attack against an employee has the MOST impact on their compliance with the organisation's "code of conduct"?

- A. Brute Force Attack.
- B. Social Engineering.
- C. Ransomware.
- D. Denial of Service.

Answer: D

NEW QUESTION 14

When handling and investigating digital evidence to be used in a criminal cybercrime investigation, which of the following principles is considered BEST practice?

- A. Digital evidence must not be altered unless absolutely necessary.
- B. Acquiring digital evidence can only be carried on digital devices which have been turned off.
- C. Digital evidence can only be handled by a member of law enforcement.
- D. Digital devices must be forensically "clean" before investigation.

Answer: D

NEW QUESTION 18

Ensuring the correctness of data inputted to a system is an example of which facet of information security?

- A. Confidentiality.
- B. Integrity.
- C. Availability.
- D. Authenticity.

Answer: B

NEW QUESTION 22

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 27

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 31

A penetration tester undertaking a port scan of a client's network, discovers a host which responds to requestsonTCP ports 22, 80, 443, 3306and 8080. What type of device has MOST LIKELY been discovered?

- A. File server.
- B. Printer.
- C. Firewall.
- D. Web server

Answer: A

NEW QUESTION 34

What advantage does the delivery of online security training material have over the distribution of printed media?

- A. Updating online material requires a single edi
- B. Printed material needs to be distributed physically.
- C. Online training material is intrinsically more accurate than printed material.
- D. Printed material is a 'discoverable record' and could expose the organisation to litigation in the event of an incident.
- E. Online material is protected by international digital copyright legislation across most territories.

Answer: B

NEW QUESTION 35

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 39

When securing a wireless network, which of the following is NOT best practice?

- A. Using WPA encryption on the wireless network.
- B. Use MAC tittering on a SOHO network with a smart group of clients.
- C. Dedicating an access point on a dedicated VLAN connected to a firewall.
- D. Turning on SSID broadcasts to advertise security levels.

Answer: C

NEW QUESTION 40

When a digital forensics investigator is conducting art investigation and handling the original data, what KEY principle must they adhere to?

- A. Ensure they are competent to be able to do so and be able to justify their actions.
- B. Ensure they are being observed by a senior investigator in all actions.
- C. Ensure they do not handle the evidence as that must be done by law enforcement officers.
- D. Ensure the data has been adjusted to meet the investigation requirements.

Answer: A

NEW QUESTION 43

What type of diagram used in application threat modeling includes malicious users as well as descriptions like mitigates and threatens?

- A. Threat trees.
- B. STRIDE charts.
- C. Misuse case diagrams.
- D. DREAD diagrams.

Answer: A

NEW QUESTION 45

What types of web application vulnerabilities continue to be the MOST prolific according to the OWASP Top 10?

- A. Poor Password Management.
- B. Insecure Deserialisation.
- C. Injection Flaws.
- D. Security Misconfiguration

Answer: C

NEW QUESTION 47

What is the first yet MOST simple and important action to take when setting up a new web server?

- A. Change default system passwords.
- B. Fully encrypt the hard disk.
- C. Apply hardening to all applications.
- D. Patch the OS to the latest version

Answer: C

NEW QUESTION 52

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 56

Which of the following is NOT considered to be a form of computer misuse?

- A. Illegal retention of personal data.
- B. Illegal interception of information.
- C. Illegal access to computer systems.
- D. Downloading of pirated software.

Answer: A

NEW QUESTION 57

Geoff wants to ensure the application of consistent security settings to devices used throughout his organisation whether as part of a mobile computing or a BYOD approach.

What technology would be MOST beneficial to his organisation?

- A. VPN.
- B. IDS.
- C. MDM.
- D. SIEM.

Answer: C

NEW QUESTION 60

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 61

Which of the following international standards deals with the retention of records?

- A. PCI DSS.
- B. RFC1918.
- C. ISO15489.
- D. ISO/IEC 27002.

Answer: C

NEW QUESTION 65

When considering the disposal of confidential data, equipment and storage devices, what social engineering technique SHOULD always be taken into consideration?

- A. Spear Phishing.
- B. Shoulder Surfing.
- C. Dumpster Diving.
- D. Tailgating.

Answer: A

NEW QUESTION 69

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 72

What term refers to the shared set of values within an organisation that determine how people are expected to behave in regard to information security?

- A. Code of Ethics.
- B. Security Culture.
- C. System Operating Procedures.
- D. Security Policy Framework.

Answer: B

Explanation:

<https://www.cpni.gov.uk/developing-security-culture#:~:text=Developing%20a%20Security%20Culture,-What>

NEW QUESTION 74

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

- 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.

Answer: D

NEW QUESTION 76

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 80

What type of attack attempts to exploit the trust relationship between a user client based browser and server based websites forcing the submission of an authenticated request to a third party site?

- A. XSS.
- B. Parameter Tampering

C. SQL Injection.
D. CSRF.

Answer: D

NEW QUESTION 83

Which membership based organisation produces international standards, which cover good practice for information assurance?

A. BSI.
B. IETF.
C. OWASP.
D. ISF.

Answer: A

NEW QUESTION 86

.....

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](#)