

BCS

Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0



NEW QUESTION 1

When establishing objectives for physical security environments, which of the following functional controls SHOULD occur first?

- A. Delay.
- B. Drop.
- C. Deter.
- D. Deny.

Answer: C

NEW QUESTION 2

Which of the following controls would be the MOST relevant and effective in detecting zero day attacks?

- A. Strong OS patch management
- B. Vulnerability assessment
- C. Signature-based intrusion detection.
- D. Anomaly based intrusion detection.

Answer: B

Explanation:

<https://www.sciencedirect.com/topics/computer-science/zero-day-attack>

NEW QUESTION 3

How does the use of a "single sign-on" access control policy improve the security for an organisation implementing the policy?

- A. Password is better encrypted for system authentication.
- B. Access control logs are centrally located.
- C. Helps prevent the likelihood of users writing down passwords.
- D. Decreases the complexity of passwords users have to remember.

Answer: B

NEW QUESTION 4

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

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

Answer: B

NEW QUESTION 5

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 6

As well as being permitted to access, create, modify and delete information, what right does an Information Owner NORMALLY have in regard to their information?

- A. To assign access privileges to others.
- B. To modify associated information that may lead to inappropriate disclosure.
- C. To access information held in the same format and file structure.
- D. To delete all indexed data in the dataset.

Answer: B

NEW QUESTION 7

What term is used to describe the act of checking out a privileged account password in a manner that bypasses normal access control 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 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

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 10

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

When preserving a crime scene for digital evidence, what actions SHOULD a first responder initially make?

- A. Remove power from all digital devices at the scene to stop the data changing.
- B. Photograph all evidence and triage to determine whether live data capture is necessary.
- C. Remove all digital evidence from the scene to prevent unintentional damage.
- D. Don't touch any evidence until a senior digital investigator arrives.

Answer: D

Explanation:

<https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>

NEW QUESTION 14

Which term is used to describe the set of processes that analyses code to ensure defined coding practices are being followed?

- A. Quality Assurance and Control
- B. Dynamic verification.
- C. Static verification.
- D. Source code analysis.

Answer: D

NEW QUESTION 17

In business continuity, what is a battle box?

- A. A portable container that holds items and information useful in the event of an organisational disaster.
- B. An armoured box that holds all an organisation's backup databases.
- C. A collection of tools and protective equipment to be used in the event of civil disturbance.
- D. A list of names and addresses of staff to be utilised should industrial action prevent access to a building.

Answer: A

Explanation:

<http://www.battlebox.biz/why.asp>

NEW QUESTION 18

Why might the reporting of security incidents that involve personal data differ from other types of security incident?

- A. Personal data is not highly transient so its investigation rarely involves the preservation of volatile memory and full forensic digital investigation.
- B. Personal data is normally handled on both IT and non-IT systems so such incidents need to be managed in two streams.

- C. Data Protection legislation normally requires the reporting of incidents involving personal data to a Supervisory Authority.
- D. Data Protection legislation is process-oriented and focuses on quality assurance of procedures and governance rather than data-focused event investigation

Answer: D

NEW QUESTION 22

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 23

How does network visualisation assist in managing information security?

- 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: D

NEW QUESTION 27

What is the name of the method used to illicitly target a senior person in an organisation so as to try to coerce them into taking an unwanted action such as a misdirected high-value payment?

- A. Whaling.
- B. Spear-phishing.
- C. C-suite spamming.
- D. Trawling.

Answer: B

NEW QUESTION 28

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

- 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: B

NEW QUESTION 31

In order to maintain the currency of risk countermeasures, how often SHOULD an organisation review these risks?

- A. Once defined, they do not need reviewing.
- B. A maximum of once every other month.
- C. When the next risk audit is due.
- D. Risks remain under constant review.

Answer: D

NEW QUESTION 34

Which of the following is NOT a valid statement to include in an organisation's security policy?

- A. The policy has the support of Board and the Chief Executive.
- B. The policy has been agreed and amended to suit all third party contractors.
- C. How the organisation will manage information assurance.
- D. The compliance with legal and regulatory obligations.

Answer: C

NEW QUESTION 35

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

- A. Updating online material requires a single edit.
- 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 39

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 40

A system administrator has created the following "array" as an access control for an organisation. Developers: create files, update files.

Reviewers: upload files, update files.

Administrators: upload files, delete files, update files. What type of access-control has just been created?

- A. Task based access control.
- B. Role based access control.
- C. Rule based access control.
- D. Mandatory access control.

Answer: C

NEW QUESTION 42

Select the document that is MOST LIKELY to contain direction covering the security and utilisation of all an organisation's information and IT equipment, as well as email, internet and telephony.

- A. Cryptographic Statement.
- B. Security Policy Framework.
- C. Acceptable Usage Policy.
- D. Business Continuity Plan.

Answer: A

NEW QUESTION 47

Which of the following statements relating to digital signatures is TRUE?

- A. Digital signatures are rarely legally enforceable even if the signers know they are signing a legal document.
- B. Digital signatures are valid and enforceable in law in most countries in the world.
- C. Digital signatures are legal unless there is a statutory requirement that predates the digital age.
- D. A digital signature that uses a signer's private key is illegal.

Answer: C

NEW QUESTION 50

Once data has been created in a standard information lifecycle, what step TYPICALLY happens next?

- A. Data Deletion.
- B. Data Archiving.
- C. Data Storage.
- D. Data Publication

Answer: A

NEW QUESTION 51

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 55

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 60

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

- 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: A

NEW QUESTION 64

Which of the following is LEAST LIKELY to be the result of a global pandemic impacting on information security?

- A. A large increase in remote workers operating in insecure premises.
- B. Additional physical security requirements at data centres and corporate headquarters.
- C. Increased demand on service desks as users need additional tools such as VPNs.
- D. An upsurge in activity by attackers seeking vulnerabilities caused by operational changes.

Answer: C

NEW QUESTION 66

Why have MOST European countries developed specific legislation that permits police and security services to monitor communications traffic for specific purposes, such as the detection of crime?

- A. Under the European Convention of Human Rights, the interception of telecommunications represents an interference with the right to privacy.
- B. GDPR overrides all previous legislation on information handling, so new laws were needed to ensure authorities did not inadvertently break the law.
- C. Police could previously intercept without lawful authority any communications in the course of transmission through a public post or telecoms system.
- D. Surveillance of a conversation or an online message by law enforcement agents was previously illegal due to the 1950 version of the Human Rights Convention.

Answer: C

NEW QUESTION 67

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 69

What are the different methods that can be used as access controls?

- * 1. Detective.
- * 2. Physical.
- * 3. Reactive.
- * 4. Virtual.
- * 5. Preventive.

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

Answer: C

NEW QUESTION 71

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 75

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

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

Answer: A

NEW QUESTION 77

What Is the KEY purpose of appending security classification labels to information?

- A. To provide guidance and instruction on implementing appropriate security controls to protect the information.
- B. To comply with whatever mandatory security policy framework is in place within the geographical location in question.
- C. To ensure that should the information be lost in transit, it can be returned to the originator using the correct protocols.
- D. To make sure the correct colour-coding system is used when the information is ready for archive.

Answer: A

NEW QUESTION 82

How might the effectiveness of a security awareness program be effectively measured?

- 1)Employees are required to take an online multiple choice exam on security principles.
- 2)Employees are tested with social engineering techniques by an approved penetration tester.
- 3)Employees practice ethical hacking techniques on organisation systems.
- 4) No security vulnerabilities are reported during an audit.
- 5) Open source intelligence gathering is undertaken on staff social media profiles.

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

Answer: C

NEW QUESTION 86

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 89

Which term describes a vulnerability that is unknown and therefore has no mitigating control which is immediately and generally available?

- A. Advanced Persistent Threat.
- B. Trojan.
- C. Stealthware.
- D. Zero-day.

Answer: D

Explanation:

[https://en.wikipedia.org/wiki/Zero-day_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))

NEW QUESTION 91

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 93

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-til-framework-and>

NEW QUESTION 96

Which of the following is a framework and methodology for Enterprise Security Architecture and Service Management?

- A. TOGAF
- B. SABSA
- C. PCI DSS.
- D. OWASP.

Answer: B

NEW QUESTION 97

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 100

.....

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](#)