

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

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 3

One traditional use of a SIEM appliance is to monitor for exceptions received via syslog. What system from the following does NOT natively support syslog events?

- A. Enterprise Wireless Access Point.
- B. Windows Desktop Systems.
- C. Linux Web Server Appliances.
- D. Enterprise Stateful Firewall.

Answer: C

NEW QUESTION 4

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 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

Which standard deals with the implementation of business continuity?

- A. ISO/IEC 27001
- B. COBIT
- C. ISO223G1.

D. BS5750.

Answer: A

NEW QUESTION 8

Which of the following is the MOST important reason for undertaking Continual Professional Development (CPD) within the Information Security sphere?

- A. Professional qualification bodies demand CPD.
- B. Information Security changes constantly and at speed.
- C. IT certifications require CPD and Security needs to remain credible.
- D. CPD is a prerequisite of any Chartered Institution qualification.

Answer: B

NEW QUESTION 9

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 10

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 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 12

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 13

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 16

Which of the following is often the final stage in the information management lifecycle?

- A. Disposal.
- B. Creation.
- C. Use.

D. Publication.

Answer: A

Explanation:

<https://timg.co.nz/blog-the-information-management-life-cycle/>

NEW QUESTION 18

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 19

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 24

Which of the following statutory requirements are likely to be of relevance to all organisations no matter which sector nor geographical location they operate in?

- A. Sarbanes-Oxley.
- B. GDPR.
- C. HIPAA.
- D. FSA.

Answer: D

NEW QUESTION 25

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 27

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 31

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 34

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 36

Which of the following is considered to be the GREATEST risk to information systems that results from deploying end-to-end Internet of Things(IoT) solutions?

- A. Use of 'cheap" microcontroller based sensors.
- B. Much larger attack surface than traditional IT systems.
- C. Use of proprietary networking protocols between nodes.
- D. Use of cloud based systems to collect IoT data.

Answer: D

NEW QUESTION 38

What Is the PRIMARY difference between DevOps and DevSecOps?

- A. Within DevSecOps security is introduced at the end of development immediately prior to deployment.
- B. DevSecOps focuses solely on iterative development cycles.
- C. DevSecOps includes security on the same level as continuous integration and delivery.
- D. DevOps mandates that security is integrated at the beginning of the development lifecycle.

Answer: C

Explanation:

<https://www.viva64.com/en/b/0710/#:~:text=DevOps%20is%20a%20methodology%20aiming,in%20the%20sof>

NEW QUESTION 39

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 44

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 47

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 mustbe done by law enforcement officers.
- D. Ensure the data has been adjusted to meet the investigation requirements.

Answer: A

NEW QUESTION 48

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 53

In a virtualised cloud environment, what component is responsible for the secure separation between guest machines?

- A. Guest Manager
- B. Hypervisor.
- C. Security Engine.
- D. OS Kernal

Answer: A

NEW QUESTION 57

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 60

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 65

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:

https://hr.nd.edu/assets/17442/behavior_model_4_ratings_3_.pdf

NEW QUESTION 70

Which of the following is LEASTLIKELY 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 72

When seeking third party digital forensics services, what two attributes should one seek when making a choice of service provider?

- A. Appropriate company accreditation and staff certification.
- B. Formal certification to ISO/IEC 27001 and alignment with ISO 17025.
- C. Affiliation with local law enforcement bodies and local government regulations.
- D. Clean credit references as well as international experience.

Answer: B

NEW QUESTION 73

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 77

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 80

In business continuity (BC) terms, what is the name of the individual responsible for recording all pertinent information associated with a BC exercise or real plan invocation?

- A. Recorder.
- B. Desk secretary.
- C. Scribe.
- D. Scrum Master.

Answer: A

NEW QUESTION 81

What is the PRIMARY reason for organisations obtaining outsourced managed security services?

- A. Managed security services permit organisations to absolve themselves of responsibility for security.
- B. Managed security services are a de facto requirement for certification to core security standards such as ISG/IEC 27001
- C. Managed security services provide access to specialist security tools and expertise on a shared, cost-effective basis.
- D. Managed security services are a powerful defence against litigation in the event of a security breach or incident

Answer: A

NEW QUESTION 85

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

Which of the following testing methodologies TYPICALLY involves code analysis in an offline environment without ever actually executing the code?

- A. Dynamic Testing.
- B. Static Testing.
- C. User Testing.
- D. Penetration Testing.

Answer: D

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 92

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 96

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 100

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 105

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 in a system.

Answer: A

Explanation:

Vulnerability

A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats.

An asset is any tangible or intangible thing or characteristic that has value to an organization, a control is any administrative, managerial, technical, or legal method that can be used to modify or manage risk,

and a threat is any potential event that could harm an organization or system. <https://www.praxiom.com/iso-27000-definitions.htm>

NEW QUESTION 110

Which of the following subjects is UNLIKELY to form part of a cloud service provision IaaS contract?

- A. User security education.
- B. Intellectual Property Rights.
- C. End-of-service.
- D. Liability

Answer: D

NEW QUESTION 112

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 113

.....

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 First Try
- * CISMP-V9 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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