



BCS

Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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 3

Which of the following is MOST LIKELY to be described as a consequential loss?

- A. Reputation damage.
- B. Monetary theft.
- C. Service disruption.
- D. Processing errors.

Answer: A

NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 10

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 15

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 20

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 21

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 22

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 23

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 28

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 31

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 32

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 37

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 38

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 40

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 44

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 45

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 48

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 53

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 57

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 59

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 60

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 61

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 68

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 72

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 73

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 75

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 80

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 84

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 87

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 91

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

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

Answer: A

NEW QUESTION 96

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 99

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

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

Answer: D

NEW QUESTION 102

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 103

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 104

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 108

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 110

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 112

James is working with a software programme that completely obfuscates the entire source code, often in the form of a binary executable making it difficult to inspect, manipulate or reverse engineer the original source code.

What type of software programme is this?

- A. Free Source.
- B. Proprietary Source.
- C. Interpreted Source.
- D. Open Source.

Answer: C

NEW QUESTION 113

.....

Relate Links

100% Pass Your CISMP-V9 Exam with ExamBible Prep Materials

<https://www.exambible.com/CISMP-V9-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>