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

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

Answer: B

NEW QUESTION 4
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 5
Which of the following is the MOST important reason for undertaking Continual Professional Development (CPD)within the Information Securitysphere?

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 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 knownprinciple.
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 largeorganisation?

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

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

Answer: B

NEW QUESTION 14
Which of the following is an accepted strategic option for dealing with risk?

A. Correction.
B. Detection.
C. Forbearance.
D. Acceptance

Answer: A

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 23
Why might the reporting of security incidents that involve personaldata differ from other types of security incident?

A. Personal data is not highly transient so its 1 investigation rarely involves the preservation of volatile memory and full forensic digitalinvestigation.
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 thandata-focused event investigation

Answer: D

NEW QUESTION 26
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 ftle format.
D. Visualisation software operates in a way that is rarely and thereby it is less prone to malware infection.

Answer: D

NEW QUESTION 28
Whatis 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 unwantedaction such as a misdirected high-value payment?

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

Answer: B

NEW QUESTION 32
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 knownvulnerabilities 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 Nrnap, Nessus and Metasploit.

Answer: B

NEW QUESTION 33
In software engineering, what does 'Security by Design??mean?

A. Low Level and High Level Security Designs are restricted in distribution.
B. All security software artefacts are subject to a code-checking regime.
C. The software has been designed from its inception to be secure.
D. All code meets the technical requirements of GDPR.

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Secure_by_design#:~:text=Secure%20by%20design%20(SBD)%2C,the%20found

NEW QUESTION 35
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 loT data.

Answer: D

NEW QUESTION 36
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 39
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 41
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 42
When undertaking disaster recovery planning, which of the following would NEVER be considered a "natural" disaster?

A. Arson.
B. Electromagnetic pulse
C. Tsunami.
D. Lightning Strike

Answer: B

NEW QUESTION 46
Which of the following is an asymmetric encryption algorithm?

A. DES.
B. AES.
C. ATM.
D. RSA.

Answer: D

Explanation:
https://www.omnisecu.com/security/public-key-infrastructure/asymmetric-encryption-algorithms.php

NEW QUESTION 50
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 55
Which of the following uses are NOT usual ways that attackers have of leveraging botnets?

A. Generating and distributing spam messages.
B. Conducting DDOS attacks.
C. Scanning for system & application vulnerabilities.
D. Undertaking vishing attacks

Answer: D

NEW QUESTION 59
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 61
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 62
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 fifes, 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 63
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 68
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 69
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-dynamicmodeling
C. Desk-top exercise.
D. Fault stressing
E. C

Answer: E

NEW QUESTION 74
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 77
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 81
In order to better improve the security culture within an organisation with a top down approach, which of the following actions at board level is theMOST effective?

A. Appointment of a Chief Information Security Officer (CISO).
B. Purchasing all senior executives personal firewalls.
C. Adopting an organisation wide "clear desk" policy.
D. Developing a security awareness e-learning course.

Answer:

A

NEW QUESTION 84
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 withISO 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 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
In business continuity (BC) terms, what is the name of the individual responsible for recording all pertinent information associated with a BCexercise or real plan invocation?

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

Answer: A

NEW QUESTION 94
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 98
Which type of facility is enabled by a contract with an alternative data processing facility which willprovide HVAC, power and communicationsinfrastructure as well 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 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 104
Which of the following compliance legal requirements are covered by the ISO/IEC 27000 series?
* 1. Intellectual Property Rights.
* 2. Protection of Organisational Records
* 3. Forensic recovery of data.
* 4. Data Deduplication.
* 5. Data Protection & Privacy.

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

Answer: D

NEW QUESTION 105
Which standards framework offers a set of IT Service Management best practices to assist organisations in aligning IT service delivery withbusiness 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-itil-framework-and

NEW QUESTION 107
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 112
James is working with a software programme that completely obfuscates the entire source code, often in the form of a binary executablemaking 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 115
......

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/