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 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 3
What form of training SHOULD developers be undertaking to understand the security of the code they havewritten and how it can improvesecurity defence whilst being attacked?

A. Red Team Training.
B. Blue Team Training.
C. Black Hat Training.
D. Awareness Training.

Answer: C

NEW QUESTION 4
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 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
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 7
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 8

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 9
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 10
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 10
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 11
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 14
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 16
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 18
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 20
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 23
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 24
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 25
What types of web application vulnerabilities continue to be the MOST prolific according to the OWASP Top 10?

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

Answer: C

NEW QUESTION 29
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 31
Which of the following is NOT aninformation 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 33
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 36
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 39
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 40
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)

NEW QUESTION 42
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 47
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 50
What type of attack attempts to exploit the trust relationship between a user client based browser and server based websites forcing thesubmission of an authenticated request to a third party site?

A. XSS.
B. Parameter Tampering
C. SQL Injection.
D. CSRF.

Answer:

D

NEW QUESTION 55
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 58
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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