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
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
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
The policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost-effectiveinfrastructure from the time information is conceived through its final disposition.
Which of the below business practices does this statement define?

A. Information Lifecycle Management.
B. Information Quality Management.
C. Total Quality Management.
D. Business Continuity Management.

Answer: A

Explanation:
https://www.stitchdata.com/resources/glossary/information-lifecycle-management/#:~:text=%E2%80%9CILM%

NEW QUESTION 5
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 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
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 8
Which security concept provides redundancy in the event a security control failure or the exploitation of a vulnerability?

A. System Integrity.
B. Sandboxing.
C. Intrusion Prevention System.
D. Defence in depth.

Answer: D

Explanation:
https://en.wikipedia.org/wiki/Defense_in_depth_(computing)

NEW QUESTION 9
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 10
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 15
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 18
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
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 25
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 27
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 30
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 33
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 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 37
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 39
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 41
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 45
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 46
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 51
Why have MOST European countries developed specific legislation that permits police and security services to monitor communications trafficfor specific purposes, such as the detection of crime?

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

Answer: C

NEW QUESTION 54
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 59
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 61
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 63
What term refers to the shared set of values within an organisation that determine how people are expected tobehave in regard to informationsecurity?

A. Code of Ethics.
B. Security Culture.
C. System Operating Procedures.
D. Security Policy Framework.

Answer: B

Explanation:
https://www.cpni.gov.uk/developing-security-culture#:~:text=Developing%20a%20Security%20Culture,-What

NEW QUESTION 68
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 73
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 74
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 76
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 81
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 82
.....

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