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
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
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 5
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 6
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 7
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 8
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 9
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 10
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 10
In business continuity, what is a battle box?

A. A portable container that holds Items and information useful in the event of an organisational disaster.
B. An armoured box that holds all an organisation's backup databases.
C. A collection of tools and protective equipment to be used in the event of civil disturbance.
D. A list of names and addresses of staff to be utilised should industrial action prevent access to a building.

Answer: A

Explanation:
http://www.battlebox.biz/why.asp

NEW QUESTION 13
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 17
Which of the following describes a qualitative risk assessment approach?

A. A subjective assessment of risk occurrence likelihood against the potentialimpact 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 arisk.
C. The use of Monte-Carlo Analysis and Layers of Protection Analysis (LOPA) to determine the overallseverity 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 22
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 25
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 27
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 28
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 30
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 33
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 35
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 36
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 38
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 42
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 43
When considering the disposal of confidential data, equipment and storage devices, what social engineering technique SHOULD always betaken into consideration?

A. Spear Phishing.
B. Shoulder Surfing.
C. Dumpster Diving.
D. Tailgating.

Answer: A

NEW QUESTION 44
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 46
Which of the following is NOT an accepted classification of security controls?

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

Answer: A

NEW QUESTION 49
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 expertiseon 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 51
By what means SHOULD a cloud service provider prevent one client accessing data belonging to another in a shared server environment?

A. By ensuring appropriate data isolation and logical storage segregation.
B. By using a hypervisor in all shared severs.
C. By increasing deterrent controls through warning messages.
D. By employing intrusion detection systems in a VMs.

Answer: D

NEW QUESTION 56
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 59
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 64
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 66
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 68
Which of the following subjects is UNLIKELY to form part of a cloud service provision laaS contract?

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

Answer: D

NEW QUESTION 70
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 73

......

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

100% Actual & Verified — Instant Download, Please Click
Order The CISMP-V9 Practice Test Here