Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0

https://www.2passeasy.com/dumps/CISMP-V9/

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
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 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
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
What term is used to describe the act of checking out a privileged account password in a manner that bypasses normal access controlsprocedures during a critical emergency situation?

A. Privileged User Gateway
B. Enterprise Security Management
C. Multi Factor Authentication.
D. Break Glass

Answer: C

NEW QUESTION 6
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 7
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 8
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 9
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 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 10
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 14
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 19
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 24
When handling and investigating digital evidence to be used in a criminal cybercrime investigation, which of the following principles isconsidered BEST practice?

A. Digital evidence must not be altered unless absolutely necessary.
B. Acquiring digital evidence cart 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 29
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 34
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 37
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 39
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 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 44
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 47
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 48
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 51
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 56
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 61
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 66
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 71
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 75
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 80
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 83
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 84
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 85
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 87
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 89
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 93
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 95
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 iin a system.

Answer: A

Explanation:
Vulnerability
A vulnerability is a weakness of an asset or control thactould potentially be exploited by one or more threats.
An asset is any tangible or intangible thing or characteristtichat has value to an organization, a control is any administrativme, anagerial, technical, or legal method that can be used to modifyor manage risk,
and a threat is any potential event that coulhdarm an organization or system. https://www.praxiom.com/iso-27000-definitions.htm

NEW QUESTION 100
......