

BCS

Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0



NEW QUESTION 1

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 2

What form of training SHOULD developers be undertaking to understand the security of the code they have written and how it can improve security defence whilst being attacked?

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

Answer: C

NEW QUESTION 3

The policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost-effective infrastructure 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%99CILM%](https://www.stitchdata.com/resources/glossary/information-lifecycle-management/#:~:text=%E2%80%99CILM%22%3A%20the%20policies%2C%20processes%2C%20practices%2C%20and%20tools%20used%20to%20align%20the%20business%20value%20of%20information%20with%20the%20most%20appropriate%20and%20cost-effective%20infrastructure%20from%20the%20time%20information%20is%20conceived%20through%20its%20final%20disposition%2C%20the%20statement%20defines%20the%20practice%20of%20information%20lifecycle%20management%20(ILM).)

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

What term is used to describe the act of checking out a privileged account password in a manner that bypasses normal access control procedures 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

Which standard deals with the implementation of business continuity?

- A. ISO/IEC 27001
- B. COBIT
- C. ISO223G1.
- D. BS5750.

Answer: A

NEW QUESTION 7

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 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_\(computing\)](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

Which security framework impacts on organisations that accept credit cards, process credit card transactions, store relevant data or transmit credit card data?

- A. PCI DSS.
- B. TOGAF.
- C. ENISA NIS.
- D. Sarbanes-Oxley

Answer: A

Explanation:

<https://digitalguardian.com/blog/what-pci-compliance>

NEW QUESTION 11

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 16

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 17

Which of the following describes a qualitative risk assessment approach?

- A. A subjective assessment of risk occurrence likelihood against the potential impact 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 a risk.
- C. The use of Monte-Carlo Analysis and Layers of Protection Analysis (LOPA) to determine the overall severity 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 18

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 file format.
- D. Visualisation software operates in a way that is rarely and thereby it is less prone to malware infection.

Answer: D

NEW QUESTION 19

In a security governance framework, which of the following publications would be at the HIGHEST level?

- A. Procedures.
- B. Standards
- C. Policy.
- D. Guidelines

Answer: A

NEW QUESTION 20

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

NEW QUESTION 21

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 IoT data.

Answer: D

NEW QUESTION 24

What advantage does the delivery of online security training material have over the distribution of printed media?

- A. Updating online material requires a single edit
- 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 29

When securing a wireless network, which of the following is NOT best practice?

- A. Using WPA encryption on the wireless network.
- B. Use MAC filtering on a SOHO network with a small 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 33

Select the document that is MOST LIKELY to contain direction covering the security and utilisation of all an organisation's information and IT equipment, as well as

email, internet and telephony.

- A. CryptographicStatement.
- B. Security Policy Framework.
- C. Acceptable Usage Policy.
- D. Business Continuity Plan.

Answer: A

NEW QUESTION 34

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 38

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 43

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 44

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 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 53

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 54

Which of the following international standards deals with the retention of records?

- A. PCI DSS.
- B. RFC1918.
- C. ISO15489.
- D. ISO/IEC 27002.

Answer: C

NEW QUESTION 59

When considering the disposal of confidential data, equipment and storage devices, what social engineering technique SHOULD always be taken into consideration?

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

Answer: A

NEW QUESTION 61

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 63

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

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

Answer: A

NEW QUESTION 64

Which of the following is NOT an accepted classification of security controls?

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

Answer: A

NEW QUESTION 68

Which of the following testing methodologies TYPICALLY involves code analysis in an offline environment without ever actually executing the code?

- A. Dynamic Testing.
- B. Static Testing.
- C. User Testing.
- D. Penetration Testing.

Answer: D

NEW QUESTION 71

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 72

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 75

Which standards framework offers a set of IT Service Management best practices to assist organisations in aligning IT service delivery with business 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-til-framework-and>

NEW QUESTION 80

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 83

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 in a system.

Answer: A

Explanation:

Vulnerability

A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats.

An asset is any tangible or intangible thing or characteristic that has value to an organization, a control is any administrative, managerial, technical, or legal method that can be used to modify or manage risk,

and a threat is any potential event that could harm an organization or system. <https://www.praxiom.com/iso-27000-definitions.htm>

NEW QUESTION 87

What type of attack attempts to exploit the trust relationship between a user client based browser and server based websites forcing the submission of an authenticated request to a third party site?

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

Answer: D

NEW QUESTION 90

James is working with a software programme that completely obfuscates the entire source code, often in the form of a binary executable making 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 93

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)