

CISMP-V9 Dumps

BCS Foundation Certificate in Information Security Management Principles V9.0

<https://www.certleader.com/CISMP-V9-dumps.html>



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

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 physical security control would be used to broadcast false emanations to mask the presence of true electromagnetic emanations from genuine 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-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)

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 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 7

Which standard deals with the implementation of business continuity?

- A. ISO/IEC 27001

- B. COBIT
- C. IS0223G1.
- D. BS5750.

Answer: A

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

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 10

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 know' principle.
- B. Verification of visitor's ID
- C. Appropriate behaviours.
- D. Access denial measures

Answer: D

NEW QUESTION 10

What is the PRIMARY security concern associated with the practice known as Bring Your Own Device (BYOD) that might affect a large organisation?

- A. Most BYOD involves the use of non-Windows hardware which is intrinsically insecure and open to abuse.
- B. The organisation has significantly less control over the device than over a corporately provided and managed device.
- C. Privately owned end user devices are not provided with the same volume nor frequency of security patch updates as a corporation.
- D. Under GDPR it is illegal for an individual to use a personal device when handling personal information under corporate control.

Answer: A

NEW QUESTION 12

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 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 20

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 24

Why might the reporting of security incidents that involve personal data differ from other types of security incident?

- A. Personal data is not highly transient so its investigation rarely involves the preservation of volatile memory and full forensic digital investigation.
- 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 than data-focused event investigation

Answer: D

NEW QUESTION 25

Which types of organisations are likely to be the target of DDoS attacks?

- A. Cloud service providers.
- B. Any financial sector organisations.
- C. Online retail based organisations.
- D. Any organisation with an online presence.

Answer: D

NEW QUESTION 28

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 30

What is 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 unwanted action such as a misdirected high-value payment?

- A. Whaling.
- B. Spear-phishing.
- C. C-suite spamming.
- D. Trawling.

Answer: B

NEW QUESTION 34

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 known vulnerabilities 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 Nmap, Nessus and Metasploit.

Answer: B

NEW QUESTION 38

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 41

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 45

Which of the following is an asymmetric encryption algorithm?

- A. DES.
- B. AES.
- C. ATM.
- D. RSA.

Answer: D

Explanation:

<https://www.omnisecu.com/security/public-key-infrastructure/asymmetric-encryption-algorithms.php>

NEW QUESTION 49

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 50

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 51

When a digital forensics investigator is conducting an investigation and handling the original data, what KEY principle must they adhere to?

- A. Ensure they are competent to be able to do so and be able to justify their actions.
- B. Ensure they are being observed by a senior investigator in all actions.
- C. Ensure they do not handle the evidence as that must be done by law enforcement officers.
- D. Ensure the data has been adjusted to meet the investigation requirements.

Answer: A

NEW QUESTION 56

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. Cryptographic Statement.
- B. Security Policy Framework.
- C. Acceptable Usage Policy.
- D. Business Continuity Plan.

Answer: A

NEW QUESTION 57

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 60

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 65

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 67

Why have MOST European countries developed specific legislation that permits police and security services to monitor communications traffic for specific purposes, such as the detection of crime?

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

Answer: C

NEW QUESTION 69

Geoff wants to ensure the application of consistent security settings to devices used throughout his organisation whether as part of a mobile computing or a BYOD approach.

What technology would be MOST beneficial to his organisation?

- A. VPN.
- B. IDS.
- C. MDM.
- D. SIEM.

Answer: C

NEW QUESTION 73

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 77

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 78

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 expertise on 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 79

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 81

A security analyst has been asked to provide a triple A service (AAA) for both wireless and remote access network services in an organization and must avoid using proprietary solutions.
What technology SHOULD they adapt?

- A. TACACS+
- B. RADIUS.
- C. Oauth.
- D. MS Access Database.

Answer: C

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 84

Which of the following subjects is UNLIKELY to form part of a cloud service provision IaaS contract?

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

Answer: D

NEW QUESTION 89

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

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISMP-V9 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CISMP-V9-dumps.html>