

# 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

For which security-related reason SHOULD staff monitoring critical CCTV systems be rotated regularly during each work session?

- A. To reduce the chance of collusion between security staff and those being monitored.
- B. To give experience to monitoring staff across a range of activities for training purposes.
- C. Health and Safety regulations demand that staff are rotated to prevent posture and vision related harm.
- D. The human attention span during intense monitoring sessions is about 20 minutes.

**Answer: D**

#### NEW QUESTION 3

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 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 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 6

As well as being permitted to access, create, modify and delete information, what right does an Information Owner NORMALLY have in regardto their information?

- A. To assign access privileges to others.
- B. To modify associated information that may lead to inappropriate disclosure.
- C. To access information held in the same format and file structure.
- D. To delete all indexed data in the dataset.

**Answer: B**

#### 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

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

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 10

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 13

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 15

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 18

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 22

When handling and investigating digital evidence to be used in a criminal cybercrime investigation, which of the following principles is considered BEST practice?

- A. Digital evidence must not be altered unless absolutely necessary.
- B. Acquiring digital evidence can 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 27

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 28

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 31

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 33

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 37

A penetration tester undertaking a port scan of a client's network, discovers a host which responds to requests on TCP ports 22, 80, 443, 3306 and 8080. What type of device has MOST LIKELY been discovered?

- A. File server.
- B. Printer.
- C. Firewall.
- D. Web server

**Answer:** A

#### NEW QUESTION 40

What is the PRIMARY difference between DevOps and DevSecOps?

- A. Within DevSecOps security is introduced at the end of development immediately prior to deployment.
- B. DevSecOps focuses solely on iterative development cycles.
- C. DevSecOps includes security on the same level as continuous integration and delivery.
- D. DevOps mandates that security is integrated at the beginning of the development lifecycle.

**Answer:** C

#### Explanation:

<https://www.viva64.com/en/b/0710/#:~:text=DevOps%20is%20a%20methodology%20aiming,in%20the%20sof>

#### NEW QUESTION 42

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 44

What is the root cause as to why SMS messages are open to attackers and abuse?

- A. The store and forward nature of SMS means it is considered a 'fire and forget service'.
- B. SMS technology was never intended to be used to transmit high risk content such as One-time payment codes.
- C. The vast majority of mobile phones globally support the SMS protocol inexpensively.
- D. There are only two mobile phone platforms - Android and iOS - reducing the number of target environments.

**Answer: B**

#### NEW QUESTION 49

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 53

What types of web application vulnerabilities continue to be the MOST prolific according to the OWASP Top 10?

- A. Poor Password Management.
- B. Insecure Deserialization.
- C. Injection Flaws.
- D. Security Misconfiguration

**Answer: C**

#### NEW QUESTION 57

Which of the following is NOT an information 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 58

Which of the following is LEAST LIKELY to be the result of a global pandemic impacting on information security?

- A. A large increase in remote workers operating in insecure premises.
- B. Additional physical security requirements at data centres and corporate headquarters.
- C. Increased demand on service desks as users need additional tools such as VPNs.
- D. An upsurge in activity by attackers seeking vulnerabilities caused by operational changes.

**Answer: C**

#### NEW QUESTION 59

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 64

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 69**

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 73**

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 76**

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 81**

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 86**

How might the effectiveness of a security awareness program be effectively measured?

- 1) Employees are required to take an online multiple choice exam on security principles.
- 2) Employees are tested with social engineering techniques by an approved penetration tester.
- 3) Employees practice ethical hacking techniques on organisation systems.
- 4) No security vulnerabilities are reported during an audit.
- 5) Open source intelligence gathering is undertaken on staff social media profiles.

- A. 3, 4 and 5.
- B. 2, 4 and 5.
- C. 1, 2 and 3.
- D. 1, 2 and 5.

**Answer: C**

**NEW QUESTION 90**

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 91**

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 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 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 96**

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 101**

.....



## 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](#)**