



**BCS**

**Exam Questions CISMP-V9**

BCS Foundation Certificate in Information Security Management Principles V9.0

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Guarantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

Which three of the following characteristics form the AAA Triad in Information Security?

- \* 1. Authentication
- \* 2. Availability
- \* 3. Accounting
- \* 4. Asymmetry
- \* 5. Authorisation

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

**Answer: D**

#### NEW QUESTION 2

What form of training SHOULD developers be undertaking to understand the security of the code they havewritten 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

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

Which standard deals with the implementation of business continuity?

- A. ISO/IEC 27001
- B. COBIT
- C. IS0223G1.
- D. BS5750.

**Answer: A**

#### NEW QUESTION 5

Which of the following is the MOST important reason for undertaking Continual Professional Development (CPD) within the Information Security sphere?

- A. Professional qualification bodies demand CPD.
- B. Information Security changes constantly and at speed.
- C. IT certifications require CPD and Security needs to remain credible.
- D. CPD is a prerequisite of any Chartered Institution qualification.

**Answer: B**

#### 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

Which of the following statutory requirements are likely to be of relevance to all organisations no matter which sector nor geographical location they operate in?

- A. Sarbanes-Oxley.
- B. GDPR.
- C. HIPAA.
- D. FSA.

**Answer:** D

#### NEW QUESTION 8

What form of attack against an employee has the MOST impact on their compliance with the organisation's "code of conduct"?

- A. Brute Force Attack.
- B. Social Engineering.
- C. Ransomware.
- D. Denial of Service.

**Answer:** D

#### NEW QUESTION 9

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 10

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 10

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 11

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 12

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 14

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 17

Which of the following statements relating to digital signatures is TRUE?

- A. Digital signatures are rarely legally enforceable even if the signers know they are signing a legal document.
- B. Digital signatures are valid and enforceable in law in most countries in the world.
- C. Digital signatures are legal unless there is a statutory requirement that predates the digital age.
- D. A digital signature that uses a signer's private key is illegal.

**Answer: C**

#### NEW QUESTION 20

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 23

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 26

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 the MOST 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 30

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 31

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 33

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 34

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 37**

.....

## Relate Links

**100% Pass Your CISMP-V9 Exam with Exam Bible Prep Materials**

<https://www.exambible.com/CISMP-V9-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>