CISMP-V9$^{Q\&As}$

BCS Foundation Certificate in Information Security Management Principles V9.0

Pass BCS CISMP-V9 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cismp-v9.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by BCS Official Exam Center

QUESTION 1

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.

Correct Answer: D

QUESTION 2

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.

Correct Answer: B

QUESTION 3

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.

Correct Answer: D

QUESTION 4

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.

Correct Answer: A

QUESTION 5

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

Correct Answer: A

QUESTION 6

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.

Correct Answer: A

QUESTION 7

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.

Correct Answer: C

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.

Correct Answer: C

QUESTION 9

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.

Correct Answer: A

https://www.stitchdata.com/resources/glossary/information-lifecycle- management/#:~:text=%E2%80%9CILM%20is%20comprised%20of%20the,(SNIA%2C%20via%20Info world).

QUESTION 10

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.

Correct Answer: A

QUESTION 11

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.

Correct Answer: A

QUESTION 12

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 known principle.

B. Verification of visitor\\'s ID

C. Appropriate behaviours.

D. Access denial measures

Correct Answer: D

QUESTION 13

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.

Correct Answer: C

QUESTION 14

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

A. Nominative.

B. Preventive.

C. Detective.

D. Corrective.

Correct Answer: A

QUESTION 15

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.

Correct Answer: B