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.leads4pass.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

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

Correct Answer: C

QUESTION 2

Which of the following controls would be the MOST relevant and effective in detecting zero day attacks?

A. Strong OS patch management

B. Vulnerability assessment

C. Signature-based intrusion detection.

D. Anomaly based intrusion detection.

Correct Answer: B

https://www.sciencedirect.com/topics/computer-science/zero-day-attack

QUESTION 3

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.

Correct Answer: D

QUESTION 4

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

Correct Answer: D

QUESTION 5

When seeking third party digital forensics services, what two attributes should one seek when making a choice of service provider?

A. Appropriate company accreditation and staff certification.

B. Formal certification to ISO/IEC 27001 and alignment with ISO 17025.

C. Affiliation with local law enforcement bodies and local government regulations.

D. Clean credit references as well as international experience.

Correct Answer: B

QUESTION 6

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.

Correct Answer: D

QUESTION 7

In business continuity, what is a battle box?

A. A portable container that holds Items and information useful in the event of an organisational disaster.

B. An armoured box that holds all an organisation\\'s backup databases.

C. A collection of tools and protective equipment to be used in the event of civil disturbance.

D. A list of names and addresses of staff to be utilised should industrial action prevent access to a building.

Correct Answer: A

http://www.battlebox.biz/why.asp

QUESTION 8

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

A. Using WPA encryption on the wireless network.

B. Use MAC tittering on a SOHO network with a smart 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.

Correct Answer: C

QUESTION 9

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.

Correct Answer: D

QUESTION 10

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.

Correct Answer: D

https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

QUESTION 11

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 12

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

Correct Answer: B

QUESTION 13

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.

Correct Answer: D

QUESTION 14

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 iin a system.

Correct Answer: A

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

QUESTION 15

Which term describes a vulnerability that is unknown and therefore has no mitigating control which is immediately and generally available?

A. Advanced Persistent Threat.

B. Trojan.

C. Stealthware.

D. Zero-day.

Correct Answer: D

https://en.wikipedia.org/wiki/Zero-day_(computing)