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

BCS Foundation Certificate in Information Security Management Principles V9.0

Pass BCS CISMP-V9 Exam with 100% Guarantee

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

QUESTION 1

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

A. Poor Password Management.

B. Insecure Deserialsiation.

C. Injection Flaws.

D. Security Misconfiguration

Correct Answer: C

QUESTION 2

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-Oxiey

Correct Answer: A

https://digitalguardian.com/blog/what-pci-compliance

QUESTION 3

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 4

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 and Privacy.

A. 1, 2 and 3

B. 3, 4 and 5

C. 2, 3 and 4

D. 1, 2 and 5

Correct Answer: D

QUESTION 5

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.

Correct Answer: D

QUESTION 6

Which standard deals with the implementation of business continuity?

A. ISO/IEC 27001

B. COBIT

C. IS0223G1.

D. BS5750.

Correct Answer: A

QUESTION 7

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 8

Which of the following subjects is UNLIKELY to form part of a cloud service provision laaS contract? A User security education.

A. Intellectual Property Rights.

B. End-of-service.

C. Liability

Correct Answer:

QUESTION 9

What are the different methods that can be used as access controls?

1.

Detective.

2.

Physical.

3.

Reactive.

4.

Virtual.

5.

Preventive.

A. 1, 2 and 4.

B. 1, 2 and 3.

C. 1, 2 and 5.

D. 3, 4 and 5.

Correct Answer: C

QUESTION 10

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

Correct Answer: C

QUESTION 11

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 12

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 Nrnap, Nessus and Metasploit.

Correct Answer: B

QUESTION 13

Which of the following is a framework and methodology for Enterprise Security Architecture and Service Management?

A. TOGAF

B. SABSA

C. PCI DSS.

D. OWASP.

Correct Answer: B

QUESTION 14

Which membership based organisation produces international standards, which cover good practice for information assurance?

A. BSI.

B. IETF.

C. OWASP.

D. ISF.

Correct Answer: A

QUESTION 15

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