DUMPSQUEEN

BCS Foundation Certificate in Information Security Management Principles V9.0

BCS CISMP-V9

Version Demo

Total Demo Questions: 10

Total Premium Questions: 100

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 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.

C. It requires the use of complex software tools to undertake this risk assessment.

ANSWER: C

QUESTION NO: 2

Which security concept provides redundancy in the event a security control failure or the exploitation of a vulnerability?

A. System Integrity.

B. Sandboxing.

C. Intrusion Prevention System.

D. Defence in depth.

ANSWER: D

Explanation:

: https://en.wikipedia.org/wiki/Defense_in_depth_(computing)

QUESTION NO: 3

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

QUESTION NO: 4

What Is the PRIMARY security concern associated with the practice known as Bring Your

Own Device (BYOD) that might affect a largeorganisation?

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

QUESTION NO: 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 withISO 17025.

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

D. Clean credit references as well as international experience.

ANSWER: B

QUESTION NO: 6

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 knownprinciple.

B. Verification of visitor's ID

C. Appropriate behaviours.

D. Access denial measures

ANSWER: D

QUESTION NO: 7

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

QUESTION NO: 8

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

QUESTION NO: 9

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 knownvulnerabilities 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.

ANSWER: B

QUESTION NO: 10

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. Printed material needs to be distributed physically.

B. Online training material is intrinsically more accurate than printed material.

C. Printed material is a 'discoverable record' and could expose the organisation to litigation in the event of an incident.

D. Online material is protected by international digital copyright legislation across most territories.

ANSWER: B