Practice Exam Questions

bcs The Chartered Institute for IT

CISMP

BCS Foundation Certificate in Information Security Management Principles

EXAMKILLER
Help Pass Your Exam At First Try

BCS

Exam CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0

Version: 3.0

[Total Questions: 100]

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

Answer: D

Question No : 2

How does the use of a "single sign-on" access control policy improve the security for an organisation implementing the policy?

A. Password is better encrypted for system authentication.
B. Access controllogs are centrally located.
C. Helps prevent the likelihood of users writing down passwords.
D. Decreases the complexity of passwords users have to remember.

Answer: B

Question No : 3

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

Question No : 4

Which of the following is often the final stage in the information management lifecycle?

A. Disposal.
B. Creation.
C. Use.
D. Publication.

Answer: A

Explanation: https://timg.co.nz/blog-the-information-management-life-cycle/

Question No : 5

Why should a loading bay NEVER be used as a staff entrance?

A. Loading bays are intrinsically vulnerable, so minimising the people traffic makes securing the areas easier and more effective.
B. Loading bays are often dirty places, and staff could find their clothing damaged or made less appropriate for the office.
C. Most countries have specific legislation covering loading bays and breaching this could impact on insurance status.
D. Staff should always enter a facility via a dedicated entrance to ensure smooth access and egress.

Answer: D

Question No : 6

Which of the following is NOT aninformation 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

Question No : 7

Which of the following international standards deals with the retention of records?

A. PCI DSS.
B. RFC1918.
C. IS015489.
D. ISO/IEC 27002.

Answer: C

Question No : 8

Which types of organisations are likely to be the target of DDoS attacks?

A. Cloud service providers.
B. Any financial sector organisations.
C. Online retail based organisations.
D. Any organisation with an online presence.

Answer: D

Question No : 9

Which of the following describes a qualitative risk assessment approach?

A. A subjective assessment of risk occurrence likelihood against the potentialimpact 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 arisk.
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

Question No : 10

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 : 11

For which security-related reason SHOULD staff monitoring critical CCTV systems be rotated regularly during each work session?

A. To reduce the chance of collusion between security staff and those being monitored.
B. To give experience to monitoring staff across a range of activities for training purposes.
C. Health and Safety regulations demand that staff are rotated to prevent posture and vision related harm.
D. The human attention span during intense monitoring sessions is about 20 minutes.

Answer: D

Question No : 12

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

Question No : 13

Once data has been created In a standard information lifecycle, what step TYPICALLY happens next?

A. Data Deletion.
B. Data Archiving.
C. Data Storage.
D. Data Publication

Answer: A

Question No : 14

Which algorithm is a current specification for the encryption of electronic data established by NIST?

A. RSA.
B. AES.
C. DES.
D. PGP.

Answer: B

Explanation: https://www.nist.gov/publications/advanced-encryption-standard-aes

Question No : 15

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 : 16

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.

Answer: C

Question No : 17

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

Question No : 18

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 & Privacy.

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

Answer: D

Question No : 19

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.

Answer: D

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

Question No : 20

A system administrator has created the following "array" as an access control for an organisation.

Developers: create files, update files.

Reviewers: upload files, update files.

Administrators: upload files, delete fifes, update files.

What type of access-control has just been created?

A. Task based access control.
B. Role based access control.
C. Rule based access control.
D. Mandatory access control.

Answer: C

Question No : 21

A security analyst has been asked to provide a triple A service (AAA) for both wireless and remote access network services in anorganizationand must avoid using proprietary solutions.

What technology SHOULD they adapt?

A. TACACS+
B. RADIUS.
C. Oauth.
D. MS Access Database.

Answer: C

Question No : 22

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.

Answer: A

Explanation: Vulnerability

A vulnerability is a weakness of an asset or control thatcould potentially be exploited by one or more threats.

An asset is any tangible or intangible thing or characteristicthat has value to an organization, a control is any administrative,managerial, technical, or legal method that can be used to modifyor manage risk, and a threat is any potential event that couldharm an organization or system.

https://www.praxiom.com/iso-27000-definitions.htm

Question No : 23

A penetration tester undertaking a port scan of a client's network, discovers a host which responds to requestsonTCP ports 22, 80, 443, 3306and 8080.

What type of device has MOST LIKELY been discovered?

A. File server.
B. Printer.
C. Firewall.
D. Web server

Answer: A