BCS Foundation Certificate in Information Security Management Principles v10.0

Specimen Paper

Record your surname / last / family name and initials on the answer sheet.

Sample paper only 20 multiple-choice questions.
Multiple choice questions allow only one correct answer to be selected for 1 mark.
1 mark awarded to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A B C or D**.
Your answers should be clearly indicated on the answer sheet.

Pass mark: 13/20
Time allowed: 30 minutes

This professional certification is not regulated by the following United Kingdom Regulators - Ofqual, Qualifications in Wales, CCEA or SQA.

1 Which of the following **correctly** describes authorisation in the context of information security?

A The unique information that distinguishes one user or device from any other.
B The process of accurately verifying the identity of a user or device.
C The right or permission that is granted to access a system resource.
D The property that ensures that any actions can be traced uniquely to a specific user.

2 Which of the following describes the main objective of the Data Protection Act 2018 in the UK?

A To replace GDPR, following Brexit, as the UK's legal framework for data protection.
B To provide specific guidelines for data retention and processing policies within the UK.
C To supplement GDPR and update data protection laws in the UK.
D To restrict individuals from accessing their personal data held by organisations in the UK.

3 Which of the following is an example of a preventive control?

A CCTV monitoring.
B Firewall.
C Incident response plan.
D Intrusion detection system (IDS).

4 Which of the following describes a valid way to identify threats to an organisation?

A Conducting regular vulnerability assessments and penetration tests.
B Monitoring employee social media activity for suspicious behaviour.
C Using quantitative methods to calculate the impact of potential threats.
D Implementing multi-factor authentication for all users across the organisation.

5 Which of the following risk analysis metrics quantifies the financial impact of an occurrence of a risk?

A Single loss expectancy (SLE).
B Annual rate of occurrence (ARO).
C Risk assessment matrix.
D Qualitative risk analysis.

6 Which of the following **best** describes the role of an information security manager?

A To deliver cyber security training sessions to employees.
B To lead and coordinate an organisation's security policy implementation.
C To develop secure software to be used by an organisation's IT department.
D To test and implement new security measures within an organisation.

7 Which of the following **correctly** explains the purpose of intellectual property protections?

A They protect sensitive personal data within an organisation.
B They protect an organisation’s original creative works.
C They deter individuals from using technology in malicious ways.
D They dictate the length of time information must be kept for.

8 Which of the following **correctly** describes a key principle of the ISO 27001 standard?

A It aims to restrict the sharing of data across countries.
B It focuses on physical security within the organisation.
C It is a risk-based approach to information security.
D Its primary aim is the encryption of all inbound and outbound data.

9 Which of the following **best** explains the concept of role-based access control?

A A system that allows users to manually request access to specific resources as needed.
B A system that allocates permission to system resources based on user seniority.
C A system that assigns access rights by creating individual permissions for each user.
D A system that manages the allocation of permissions to resources based on job role.

10 Which of the following is **not** a step specifically involved in the threat modelling process?

A Identifying risks.
B Assessing impact.
C Training employees.
D Implementing mitigation measures.

11 Which of the following **correctly** describes the three categories of authentication factor that can be used in multi-factor authentication?

A Something you are, something you see, and something others know.
B Something you share, something you trust, and something you know.
C Something you are, something you can hold, and something you see.
D Something you are, something you have, and something you know.

12 Which stage of the data lifecycle **typically** includes storing data offline, often to meet compliance requirements?

A Archive.
B Destruction.
C Storage.
D Creation.

13 Which of the following **correctly** describes how a secure by design approach helps to produce secure software?

A By ensuring software is produced that will never have any vulnerabilities.
B By ensuring security is not an afterthought that has to be added at the end.
C By reducing the number of lines of code produced, thereby reducing the risk.
D By speeding up the development process, thereby avoiding coding mistakes.

14 Which type of network specifically uses technology based on the IEEE 802.11 standard and allows devices to connect via an access point?

A Local area network (LAN).
B Metropolitan area network (MAN).
C Wide area network (WAN).
D Wireless local area network (WLAN).

15 Which of the following describes an advantage of a star network topology?

A Failure of one device does not affect the others.
B It requires less cable than other topologies.
C Each device has a direct link to all the others.
D Data can be routed through multiple paths.

16 Which security strategy operates on the principle that the network is inherently hostile?

A Zero access.
B Zero day.
C Zero privilege.
D Zero trust.

17 Which of the following physical security controls is **least likely** to prevent unauthorised access?

A Motion detectors.
B Electronic door locks.
C Cages around equipment.
D Trained security guards.

18 Which of the following **correctly** describes a security incident, as defined by the NIST 800-61 incident response framework?

A Any unauthorised physical access to protected sites.
B The act of violating an explicit or implied security policy.
C The attempted or actual access to protected systems.
D Any computer event that is unexpected or unplanned.

19 One of the key disaster recovery resiliency metrics is recovery time objective (RTO). Which of the following **correctly** describes RTO?

A The longest period between outages that an organisation has experienced.
B The maximum acceptable amount of time that a system can be down.
C The maximum acceptable amount of data loss, measured in time.
D The shortest period that a business process can be inoperative.

20 Which of the following **best** explains the ethical considerations of artificial intelligence (AI) development?

A AI models that are poorly developed or trained have the potential to cause harm to society.
B It is not possible to create legislation to control the use of AI, so ethics must fill the gap.
C AI can only be used in ways that benefit society, so ethical concerns are minimal.
D Inefficient AI models can slow down data processing and reduce system performance.

End of Paper

BCS Foundation Certificate in Information Security Management Principles v10.0

Answer Key and Rationale

Question	Answer	Rationale	Syllabus Section
1	**C**	Authorisation is the process of granting appropriate rights to a user or device so they are able to access a system resource.	1.1
2	**C**	The Data Protection Act 2018 enacts the GDPR's requirements into UK law, with additional provisions for law enforcement and national security, ensuring data protection standards are upheld after Brexit.	1.3
3	**B**	Firewalls are used to prevent unauthorised access, making them preventive controls.	2.1
4	**A**	Vulnerability assessments and penetration tests are key to identifying both internal and external security weaknesses that could be exploited.	2.2
5	**A**	Single loss expectancy calculates the expected monetary loss from a single risk event.	2.2
6	**B**	The information security manager is responsible for ensuring the organisation's security strategy is implemented. They coordinate risk management efforts and ensure that the organisation's security posture aligns with its goals.	3.1
7	**B**	Intellectual property rights are the legal protection for original creative works. In the UK, they are covered under the Copyright, Designs and Patents Act 1988.	3.2
8	**C**	ISO 27001 employs a risk-based approach to people, processes and technology, allowing organisations to implement information security controls based on specific risks.	3.3
9	**D**	Role-based access control assigns access permissions according to predefined job roles within the organisation. This ensures that users only have access to the resources necessary for their role, simplifying permission management and enhancing security.	4.1
10	**C**	Threat modelling is a structured approach used to identify, quantify, and address the security risks associated with an application or system. While employee awareness and training are a vital part of effective information security, they are not specifically a part of the threat modelling process.	4.2
11	**D**	Authentication factors classically fall into the following three categories: something you know e.g. password, something you have e.g. a phone, and something you are e.g. biometric, like a fingerprint.	4.4

Question	Answer	Rationale	Syllabus Section
12	**A**	Archived data is typically no longer active and can be stored offline for long-term storage. Data is often archived as it is required to be retained for compliance purposes.	5.1
13	**B**	Secure by design is a security approach in software and system development where security considerations are integrated from the very beginning of the design process. This method ensures that security features and best practices are embedded into the architecture and design of a system rather than being added later as an afterthought.	5.2
14	**D**	Wireless LANs (WLANs) use Wi-Fi, which is based on the IEEE 802.11 standard. Wireless devices connect to a network via an access point.	6.1
15	**A**	In a star network, all devices are connected to a central hub or switch making it easy to manage and troubleshoot. Failure of one device does not affect the others.	6.1
16	**D**	Zero trust sees the network as hostile, removing trust. This approach means that no user or system, whether inside or outside the network, is inherently trusted.	6.2
17	**A**	Monitoring and detection tools such as motion detectors can be installed to alert and record that physical security has been compromised. They may act as a deterrent, but will not prevent access, whereas the other controls listed are more likely to.	7.1
18	**B**	According to the NIST 800-61 framework, a security incident is: '...the act of violating an explicit or implied security policy.'	8.1
19	**B**	RTO is the maximum acceptable amount of time that a system, application, or process can be down after a failure or disaster before normal operations must be resumed. It determines the time frame within which business functions must be restored to avoid unacceptable consequences.	8.2
20	**A**	Ethical considerations extend beyond legal compliance, addressing the broader societal impacts of AI systems and ensuring development and usage respect individuals' rights and dignity.	9.1