BCS Level 4 Certificate in Cyber Security Introduction
QAN 603/0830/8

Specimen Paper

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

Specimen paper only 20 multiple-choice questions – 1 mark awarded to each question. Mark only one answer 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 is 13/20.

Copying of this paper is expressly forbidden without the direct approval of BCS, The Chartered Institute for IT.

This qualification is regulated by Ofqual (in England).

1 Which of the following **BEST** describes an information asset?

A Any data or device that supports business processes or operations.
B A technical subject matter expert.
C An organisation's central database server.
D All hardware and software owned by an organisation.

2 A business that processes large amounts of personally identifiable information (PII) suffers a significant security incident. What is the **MOST LIKELY** type of impact?

A Regulatory.
B Operational.
C Motivational.
D Financial.

3 How does cyber security **BEST** support the UK's consumers?

A By ensuring cyber criminals outside the UK are caught.
B By making the UK a safe place in which to shop online.
C By allowing UK consumers to freely share their personal details.
D By stopping commercial organisations from overcharging consumers.

4 From a cyber security perspective, what is the relationship between risk, threat and vulnerability?

A Vulnerability is the destruction or damage to an asset after a risk calculation has been taken to mitigate against such a threat.
B A threat is when an asset might be susceptible to damage when a vulnerability has been discovered and the risk calculated.
C Risk is the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.
D There is a maximum risk when no vulnerability or threat exist.

5 In order for an organisation to be secure against a determined attack, how many risks must be successfully treated?

A All.
B Most.
C Some.
D None.

6 Which of the following is an organisation **MOST LIKELY** to be at risk from as a result of poor software maintenance practices?

A Increased likelihood of attack.
B Vulnerability to newly discovered exploits.
C High operational costs.
D Increased staff turnover.

7 The network security monitoring function of an organisation is outsourced to a third-party. What type of risk treatment is this?

A Accept.
B Avoid.
C Mitigate.
D Transfer.

8 Which assurance provides confidence in the processes applied during the development of a product, service or system?

A Intrinsic.
B Extrinsic.
C Implementation.
D Operational.

9 Which of the following is a **PRIMARY** benefit of automated vulnerability scanning as an extrinsic assurance method?

A Rapidly identify unknown vulnerabilities across multiple systems.
B Rapidly identify known vulnerabilities across multiple systems.
C Rapidly identify known vulnerabilities for an unknown system.
D Rapidly identify unknown vulnerabilities for a single system.

10 Security requirements for a new product or system are **GENERALLY** driven from which of the following?

A Security solutions.
B Security objectives.
C Security functions.
D Security guidelines.

11 A remote-access server is configured to allow Telnet connections, of the below options which **BEST** describes the vulnerability this represents?

A Low quality traffic filtering.
B Absence of access controls.
C Inadequate patch management.
D Insecure protocol usage.

12 Which of the following is **TYPICALLY** a feature of a thick client?

A It uses a server for the main processing activity.
B It does the bulk of the processing activity rather than the server.
C It is designed for use by very inexperienced people.
D It uses web-based software through the terminals.

13 A database administrator uses their privileged access to read sensitive HR files relating to other employees. What type of insider threat is being described?

A Negligent insider.
B Insider collusion.
C Malicious insider.
D Third-party insider.

14 In order for a threat to pose a valid risk to an organisation, it must have which of the following?

A Means, method and money.
B Money, manpower and motive.
C Method, opportunity and motive.
D Opportunity, manpower and money.

15 Which of the following actions **BEST** describes a preventative control?

A It instructs a user to do something in a particular way.
B It stops a user from doing the wrong thing.
C It identifies if a user has done something wrong.
D It corrects the erroneous input from a user.

16 Which industry sector developed PCI DSS?

A Manufacturing.
B Financial.
C Central government.
D Health.

17 An organisation that wants to directly store and handle customer credit card information would get the **MOST** benefit from obtaining which industry standard accreditation?

A PCI-DSS.
B Cyber Essentials.
C ISO27001.
D ISO9001.

18 Under the General Data Protection Regulation (GDPR), which of the following conditions allows data to be transferred outside of the European Economic Area (EEA)?

A Destination country is approved by European Commission.
B Data processor makes application to European Commission.
C Data can be sent cross border with no conditions.
D Data can never be sent outside of the EEA.

19 What is horizon scanning?

A Looking at developments in technology to try and identify future trends or issues.
B Identifying known threats appearing on the boundaries of a company's network.
C Determining what new inventions in technology your competitors are bringing to market.
D Scanning for vulnerabilities in the software that has been installed on the company's networks.

20 Which of the following **BEST** describes a technology that will have a major impact on the security of home-based devices in the future?

A SCADA.
B Internet of Things (IoT).
C Whaling.
D Public Key Infrastructure (PKI).

-End of Paper-