BCS Foundation Certificate in Information Security Management Principles

Specimen Paper A

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

This is a specimen paper only. The full exam is 100 multiple choice questions with a pass mark of 65/100.

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

1 Quantitative risk assessment is…

A A mandatory audit requirement.
B A numerical means to measure comparative risks.
C Demanded by ISO/IEC 27001.
D Only really possible with a computer-based analysis package.

2 The major purpose of information security in an organisation is…

A Implementing controls to reduce risks.
B Ensuring that confidentiality of information is not breached.
C Ensuring that computer systems are not hacked.
D Supporting the effective and efficient achievement of the organisation's business objectives.

3 Most security breaches caused by employees are through…

A Errors.
B Fraud.
C Physical damage to equipment.
D Malicious attacks.

4 Which of the following **BEST** describes business impact?

A The effect on an organisation of a vulnerability being exploited.
B The probability of a vulnerability being exploited against an organisation.
C The effect on an organisation of the controls being adopted.
D The number of vulnerabilities exploited in a given period.

5 Writing a security policy is important because…

A The ISO/IEC 27000 series requires it as part of its set of security documentation.
B The organisation's Board of Directors knows the issues.
C It sets out the organisation's formal stance on security for staff and contractors to see.
D It ensures the security officer knows what they should be doing.

6 The **BEST** approach to risk assessment is to…

A Compile a risk register against all information assets.
B Send a questionnaire on perceived risks to all staff.
C Employ an experienced external consultant.
D Run a risk assessment software package.

7 Information which can be proved true through observation, documents, records, or personal interview is called…

A Objective evidence.
B Corrective action.
C A non-conformity.
D An opportunity for improvement.

8 The **MOST** common cause of many internal security incidents is…

A Poor recruitment processes.
B Lack of security operating procedures.
C Inadequate network protection measures.
D Lack of awareness on the part of staff.

9 An example of a control which helps to protect against unintentional disclosure of information is…

A Regular incremental and full backups.
B A formal disciplinary process.
C Classification labelling of information.
D Independent review of information security.

10 Useful additions to a security training programme for all staff members are…

A Links to vendor agnostic websites specific to information security.
B White papers written by subject matter experts in information security.
C Vendor brochures specific to information security.
D Copies of textbooks specific to information security.

11 Computer viruses are…

A Only a problem with internet connected systems.
B Potentially very serious.
C A nuisance.
D Easily detectable.

12 With respect to security, a third party connection contract should specify…

A All the agreed security requirements of each party.
B Total compliance with ISO/IEC 27000 series.
C ISO/IEC 27000 series certification.
D A common security policy.

13 Non repudiation…

A Protects against the disclosure of information to unauthorised users.
B Protects against a person denying later that a communication or transaction took place.
C Assures that a person or system is who or what they claim to be.
D Protects against unauthorised changes in data whether intentional or accidental.

14 Computer terminals in a stock, shares and bonds dealing room are set up to allow quick acceptance of trades. Which of the following would be the **MOST** sensible safeguard to limit loss through errors?

A Thorough staff training in the need to be careful.
B Separate authorisation of all trades.
C Confirmation of all trades before committing.
D Confirmation of trades which are over a set value.

15 Penetration testing is used primarily…

A By hackers.
B To test physical security.
C By computer operators.
D By security specialists.

16 A trapdoor is…

A A structured programming technique.
B A generally unknown exit out of or entry into a program.
C A network programming technique.
D A programming technique used in real-time systems.

17 What physical control system should be considered to prevent unauthorised access, damage and interference to IT services?

A Closed Circuit TV cameras and alarm systems.
B Defined security procedures.
C A gate access control system requiring a security token.
D A physical security policy.

18 An example of a record of Information Security Management System operation is…

A A clear desk policy.
B A formal disciplinary process.
C Business continuity plan test results.
D The procedure for technical conformity checking.

19 For remote access into a company server containing personal information, the one thing all solutions will have in common is…

A A virtual private network (VPN).
B Strong authentication.
C Encryption.
D An approved gateway.

20 When setting up a contract with a supplier for hosting cloud services, which of the following safeguards is most important?

1) The ability to recover all information from the cloud if the contract is terminated.
2) The confidentiality and integrity of downloading information from the cloud.
3) The make of hardware used by the hosting supplier.
4) The service level requirement for availability of the information.

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

-End of Paper-