Making IT good for society

BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards

QAN 603/0855/2

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 qualification is regulated by Ofqual (in England).

1 Which of the following is **NOT** considered an element of information security governance?

A Managing risks appropriately.
B Managing resources efficiently and effectively.
C Measuring performance.
D Monitoring storage capacity.

2 Which of the following would you expect to form part of an information security governance framework?

a) The Main Board.
b) The Risk Management Committee.
c) The HR Committee.
d) The Information Security Management Board.

A a, b and c only.
B a, b and d only.
C c and d only.
D a and b only.

3 Which of the following **BEST** describes the term risk in respect of information security management?

A The probability of a loss tied to an asset.
B The cost of replacing an asset.
C The loss of reputation following an incident.
D The cost of legal procedure following an incident.

4 How can organisations embed security into project management practices?

A Create security milestones for defined stages of the project.
B Define the security concept at the end of the project.
C Leave the security concept to a separate project.
D Have a named individual responsible for the security concept.

5 Which action would **BEST** help an organisation meet multiple legal and regulatory requirements?

A Implement privacy training.
B Encrypt all files at database level.
C Obtain ISO 27001 certification.
D Outsource monitoring to a private Security Operations Centre.

6 Which principle is applied to ensure that only the necessary access to accomplish an assigned task is provided to users, or processes acting on behalf of users?

A Need to restrict.
B Role-based access.
C Least privilege.
D Control enhancement.

7 Which components of an organisation's internal environment does a security policy apply to?

a) Management.
b) Employees.
c) Customers.
d) Contractors.

A a, b and c only.
B b, c and d only.
C a, b and d only.
D a, c and d only.

8 Which components would be affected by the information security policy of a central government organisation?

a) Employees.
b) Shareholders.
c) Management.
d) Electorate.

A a and b only.
B b and d only.
C c and d only.
D a and c only.

9 Which legislation applies to UK companies listed on US stock exchanges?

A Health Insurance Portability and Accountability Act 1996.
B The Third Basel Accord.
C Sarbanes-Oxley Act 2002.
D Federal Information Security Management Act 2002.

10 Which public authority does NOT require a data protection officer (DPO)?

A A court acting in a judicial capacity.
B The DSS when investigating fraudulent claims.
C An NHS trust.
D The Independent Police Complaints Commission.

11 Which role would be expected to be undertaken by an independent, external party?

A ISO 27001 lead auditor.
B SOC manager.
C CISO.
D Crypto controller.

12 Which role is carried out by a CHECK team leader?

A Penetration tester.
B Lead ISO 27001 auditor.
C Information security manager.
D Security architect.

13 Which role would **NORMALLY** be undertaken by a permanent member of internal staff?

A Compliance manager.
B Penetration tester.
C ISO 27001 auditor.
D Vulnerability assessor.

14 Who has the authority to intercept a private communication in the UK according to the Regulation of Investigatory Powers Act 2000?

A No one has that right.
B A person with a right to control the operation or the use of a private telecommunications system.
C Only a police officer or someone acting in defence of the realm.
D A person working as a senior manager of the public telecommunications system used for the transmission.

15 What is the purpose of ISO/IEC 27001:2013?

A To provide requirements for an information security management system.
B To establish a risk management methodology to protect information assets.
C To establish guidelines for organisational information security standards and information security management practice.
D To select controls within the process of implementing an Information Security Management System.

16 In ISO 27001, what are the documentation requirements based on?

a) The size of the organisation and its activities, processes and services.
b) The complexity of processes and their interactions.
c) The competence of persons.
d) The need for the structure to be the same for all organisations.

A a, b and c only.
B a, b and d only.
C b, c and d only.
D a, c and d only.

17 Indicate the answer that describes the statement and reason.

Statement: An external auditor is required to certify an organisation against ISO/IEC 27001.

Reason: Certification against ISO/IEC 27001 is likely to ensure compliance with ISO/IEC 27002.

A The statement and reason are both true.
B The statement and reason are both false.
C The statement is true, and the reason is false.
D The statement is false, and the reason is true.

18 Which of the following are potential benefits to an organisation achieving ISO27001 certification?

a) Helps to keep confidential information secure.
b) Provides a competitive commercial advantage.
c) Demonstrates that products are thoroughly tested.
d) Protects company directors and shareholders.

A a, b and c only.
B a, c and d only.
C a, b and d only.
D b, c and d only.

19 Under GDPR, the relevant supervisory authority only needs to be notified of a breach when it is likely to have which of the following effects?

A Start a denial of service attack.
B Be reported in the press.
C Cause a financial loss of >€1M.
D Result in a risk to the rights and freedoms of individuals.

20 Under Data Protection Act 1998 who **SHOULD** notify the relevant parties of a security breach?

A Information commissioner.
B Data controller.
C Whoever discovered it.
D Chief executive officer.

-End of Paper-