BCS Level 3 IT Solutions Technician EPA Knowledge Unit Security and Legislation

Specimen Paper

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

Specimen paper only 10 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.

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

This knowledge unit is regulated by the following United Kingdom Regulator – NSAR.

1   To which of the following is one legally obliged to comply?

A   Legislation.
B   Corporate policies.
C   Standards.
D   Professional ethics.

2   Which of the following is **NOT** an offence under the Computer Misuse Act?

A   Unauthorised access with intent to commit further offences.
B   Unauthorised access to computer material.
C   Unauthorised modification of computer material.
D   Unauthorised manipulation of computer users.

3   Why is the ISO 27000 family of standards important?

A   It is applicable across business sectors and is recognised globally.
B   It supports the ISO 9000 quality standard.
C   It originated in the UK.
D   Its origins in the USA ensure it has international acceptance.

4   Which international standard can be used to demonstrate to legislators, regulators and other interested parties that a business is adhering to good practice in business continuity management?

A   ISO 27001.
B   ISO 14001.
C   ISO 22301.
D   ISO 9001.

5   What is the **PRIMARY** benefit of business continuity planning?

A   It reduces the probability of external threats manifesting.
B   It reduces the risk of harm to an organisation in the event of system outages.
C   It ensures full duplication of all systems to allow immediate cut-over in the event of a disaster.
D   It removes the threat of damage from natural causes such as floods and fires.

6   Which of the following would be described as a 'technology' security control?

A   Business continuity management.
B   ISO 27001.
C   Security awareness training.
D   Firewall.

7   Which of the following is the **MOST** important element of any cyber security awareness initiative?

A   High quality graphical delivery.
B   Interactive online training.
C   Management leading by example.
D   A weekly email newsletter.

8   What group of people are **MOST LIKELY** to cause a security incident?

A   Insiders.
B   Hackers.
C   Foreign intelligence services.
D   Serious and organised criminal gangs.

9   What is the term used to describe the process of updating a system or device to eliminate bugs and potential weaknesses?

A   Data loss prevention.
B   Default system reset.
C   Full disk encryption.
D   Patching.

10   Which two terms are the core components of a risk?

A   Threat and likelihood.
B   Impact and likelihood.
C   Impact and vulnerability.
D   Vulnerability and harm.

End of Paper