BCS Level 4 Award in Security Technology Building Blocks QAN 603/0884/9

Specimen Paper

Version 4.0
July 2020

Change History

Any changes made to the specimen paper shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
Version 1.0 November 2016	Document created.
Version 2.0 November 2017	Questions edited to fit enhanced syllabus
Version 3.0 October 2019	Major changes to questions to match Syllabus question weightings.
Version 4.0 July 2020	Major changes to questions to match updated syllabus (V3.0). Paper size reduced. Title page, change history table and related syllabus section added.

Related Syllabus

This sample paper and answer key are related to the following syllabus:

BCS Level 4 Award in Security Technology Building Blocks Syllabus V3.0 March 2020

BCS Level 4 Award in Security Technology Building Blocks QAN 603/0884/9

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 for 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.

This is a specimen examination paper only.

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 would be implemented on a server to **BEST** protect documents stored at rest?

A File integrity monitoring.
B File encryption.
C Traffic encryption.
D Anti-malware software.

2 Which of the following statements is TRUE for the process of mutual authentication?

A Two remote systems authenticate each other at the same time.
B Two remote systems authenticate each other in sequence.
C Three or more remote systems authenticate each other at the same time.
D Three or more remote systems authenticate each other in sequence.

3 A user who does not usually do remote working needs to work on some documents over the weekend. They have been given permission to copy the documents onto a USB stick to take home. Which of the following would be the **BEST** solution to ensure any files saved to the USB stick are not compromised in the event it is lost?

A Removable media encryption.
B Data loss prevention.
C Trusted platform module
D File encryption.

4 An appropriate level of which of the following would **BEST** provide protection against a man-in-the-middle attack?

A File encryption.
B Device encryption.
C Traffic encryption.
D Database encryption.

5 A public facing website using HTTPS is likely to first deter a potential attacker at which stage of the MITRE ATT&CK chain?

A Initial access.
B Execution.
C Persistence.
D Exfiltration.

6 Educating users to guard against spear phishing is an example of a defence against which stage of the MITRE ATT&CK chain?

A Initial access.
B Privilege escalation.
C Defence evasion.
D Credential access.

7 When selecting a payment processor to take credit card payments, which accreditation would be **MOST** important for the processor to hold?

A ISO-27001:2013.
B Cyber Essentials +.
C CREST.
D PCI-DSS.

8 A supplier is ISO27001 certified. Which of following are they **LEAST LIKELY** to have in place?

A The ability to securely take card payments.
B An annual penetration testing programme.
C An appropriate process controlling user authentication.
D Antivirus software that updates daily.

9 Which of the following, if not enabled, could lead to a man-in-the-middle attack?

A Network firewall.
B Traffic encryption.
C DNS filtering.
D Data loss prevention.

10 Which of the following is **MOST LIKELY** to be a benefit of an open source security solution?

A Products are more scalable.
B Products are more stable.
C Products have better support.
D Products are highly editable and configurable.

-End of Paper-