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

Specimen Paper Answer Key

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 to 20 questions. 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

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**B**	Data at rest should be encrypted and file encryption is the only method listed that would achieve this.	1.1
2	**A**	During mutual authentication, both remote systems authenticate each other at the same time.	1.1
3	**A**	Encrypting the whole media would ensure all documents saved to the stick would be protected.	1.2
4	**C**	Traffic encryption such as TLS when appropriately configured prevents against man-in-the-middle attacks.	1.2
5	**A**	HTTPS may deter an attacker at the initial access stage of an attack as the traffic would be encrypted making their task much harder. They may then choose another approach or a different target. HTTPS could also deter an attacker at a later stage in the attack, however, initial access is the first stage.	1.3
6	**A**	All types of phishing are a mechanism for getting a foot-in-the-door for attackers.	1.3
7	**D**	Without PCI-DSS a company is not allowed to process card payments.	1.4
8	**A**	ISO27001 does not provide any assurances for card payments, but does require user access control, appropriate antivirus and vulnerability management.	1.4
9	**B**	Appropriate traffic encryption would prevent an attacker from reading the network traffic to then be able to misuse it.	1.5
10	**D**	Open source solutions are often highly editable / configurable. The other options are attributable to commercial off-the-shelf solutions, but they are usually not customisable to the degree of open source.	1.6