BCS Level 4 Award in Security Principles
Answer Key and Rationale – QAN 603/3255/4

Question	Answer	Explanation / Rationale	Syllabus Sections
1	D	Voice over IP is the only voice-based application protocol in the list and is used across public and private packet switched networks like 3G / 4G, wireless LANs, Ethernet, WANSs etc. It can be both secure and insecure.	1.2
2	B	Threat intelligence, also known as cyber threat intelligence (CTI), is organised, analysed and refined information about potential or current attacks that threaten an organisation.	1.5
3	B	Plain text is taken by the sender as an input and is encrypted into cipher text as an output (which makes it unreadable and hence confidentiality is ensured), and the receiver decrypts the cipher text as an input back into plain text as an output.	1.3
4	C	Apprentices should be able to differentiate between operating systems from major vendors.	1.1
5	A	Android is a stack of software applications for mobile devices, which includes an operating system, middleware applications, and some key applications.	1.1
6	A	National CERTs (Computer Emergency and Response Team) are generally responsible for collating and disseminating cyber threat intelligence to a nations citizens, businesses and other interested parties. They provide a central point for organisations and individuals to be able to identify what current threats might affect an organisation in the future and what needs to be done to prevent an incident.	1.5
7	B	By employing spam filtering phishing emails might not be received as they are often unsolicited and in a common format. Web filters will remove access to URLS which are known to contain phishing sites. Turning off HTML often renders some phishing emails inoperative and / or reveals the hidden links.	1.4
8	A	Authentication is about identifying who is issuing the command and making sure that the caller is really that person / system. Authorisation occurs necessarily after, since it is about deciding whether the duly authenticated requester should be allowed to proceed or not. Auditing usage happens after the user has logged in.	1.3
9	D	A sandbox will stop the ransomware malware application that runs the executable from being able to encrypt user files.	1.4
10	A	VPNs add confidentiality across the network tunnel (created across a shard infrastructure) they do this by creating a secure network.	1.2

Copyright © BCS 2018