BCS Level 4 Certificate in Cyber Security Introduction
Answer Key and Rationale QAN 603/0830/8

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	Information assets cover data and devices used by an organisation. People are usually considered information assets but people, devices or data alone is not the best answer.	1.1
2	**A**	Breaches involving personally identifiable information (PII) typically attract large regulatory fines and penalties from the ICO under regulations such as the GDPR and Data Protection Act. Although the other options could be valid, in this case they are likely to be secondary to regulatory impact.	1.3
3	**B**	Cyber security makes the UK a safe place to shop online by helping to prevent fraud and identity theft. Ensuring criminals outside the UK are caught may be a consequence but it is not the main benefit. Consumers can share their information in whatever ways they choose, and cyber security may prevent unlawful access to that data.	1.5
4	**C**	'Risk' is the potential result of a threat impacting negatively on assets – normally via a vulnerability or weakness. A risk is derived from vulnerabilities. If there is no vulnerability, there is no risk. If there is no threat, there is no risk.	2.2
5	**A**	Due to the asymmetry between risks and exploits, for an organisation to be totally secure against any attacker, all risks must be treated. An attacker only needs to exploit a single risk to subvert the security controls of an organisation.	2.4
6	**B**	Poor or absent patch management hygiene exposes an organisation to significant vulnerability to any new exploits that are identified for older software versions, as is a regular occurrence for popular software applications. Likelihood of attack could increase but is a by-product of the vulnerability. Costs and turnover are not risk factors related to system maintenance.	2.6
7	**D**	Using a third party transfers some or most residual risk to the third party from the organisation based on agreed service-levels. All other options are invalid for this scenario.	2.8
8	**A**	Intrinsic assurance relates to how a system is built. Factors considered can include the professional qualifications of the engineers who built the system, the level and credibility of review and the presence (or otherwise) of an appropriate quality management system.	3.2

Question	Answer	Explanation / Rationale	Syllabus Sections
9	**B**	Automated vulnerability scanning is a quick method for identifying previously discovered (known) vulnerabilities across multiple systems in parallel, saving time and effort compared to manual black-box penetration testing approaches.	3.4
10	**B**	Security requirements are generally driven by the security objectives of a product / system. Security context / environment and threats analysis are also fed in the elicitation of security requirements. On the basis of security requirements, security functions are identified, security solutions are chosen, and security guidelines are prepared.	4.1
11	**D**	Telnet is a well-known insecure protocol which communicates data in clear-text and was succeeded by SSH many years previously.	5.1
12	**B**	If all software is installed on the device, it is a thick client, and this will require significant processing power. A thin client is a terminal connected to a server, where the device itself has very limited processing power, and the server runs the software. There is no link to the ability of the users. The use of web-based software is common to both models but usually a feature of thin clients.	5.3
13	**C**	The use of legitimate access to willingly perform a prohibited act is classified as malicious insider attack type. Negligent insiders are typically unaware they have caused a security breach and collusion, or third-party insiders require multiple individuals to perform a successful attack.	6.2
14	**C**	In order to be realised, all cyber threats require a method (the attack techniques), a motive (political, espionage or financial) and an opportunity (poor perimeter controls, lack of user awareness, vulnerable applications). Money, means and manpower are not traditionally factors in threat realisation.	6.4
15	**B**	Stopping the user doing something wrong is a preventative control e.g. blocking access to a particular website. Requiring the user to do something in a particular way is a directive control. Correcting an erroneous entry by a user is a corrective control. Identifying a user has done something wrong is a detective control.	7.1
16	**B**	Payment Card Industry - Data Security Standard (PCI - DSS) originates within the financial sector and relates to a specific area of finance – card payments.	8.1
17	**A**	All companies that handle payment card information are required to obtain PCI-DSS accreditation by most major card companies in order to reduce fraud. An organisation not achieving this accreditation is unlikely to be able to support the required business functions needed to handle such data.	8.3

Question	Answer	Explanation / Rationale	Syllabus Sections
18	**A**	Article 45 of the GDPR regulation outlines the requirement for any third-party country to have been assessed and approved by the European Commission to ensure its security and data protection laws and procedures are adequate to ensure the continued protection of data from the European Union.	8.5
19	**A**	Horizon scanning is a process which uses the idea of looking as far ahead as possible to look for trends, developments, research and related areas to help predict what threats we might face in the future. The OECD definition of horizon scanning is "a technique for detecting early signs of potentially important developments through a systematic examination of potential threats and opportunities, with emphasis on new technology and its effects on the issue at hand." http://www.oecd.org/site/schoolingfortomorrowknowledgebase/futuresthinking/overviewofmethodologies.htm	9.1
20	**B**	The Internet of things (IoT) is the extension of Internet connectivity into consumer devices and everyday objects – including those in the home. The security of these devices can have an impact on the security of the other devices attached to the same network.	10.1