BCS Level 4 Certificate in Security Case Development and Design Good Practice
Answer Key and Rationale – QAN 603/0904/0

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	Defence in depth ensures there are compensating controls in the event another control fails. Open design and economy of mechanism will not help in this situation. Fail-safe defaults would prevent users bypassing the control.	1.1
2	**A**	Fail securely ensures that if a system fails it reverts to a secure state (e.g. denies access). This prevents application-errors that may reveal system information or data.	1.1
3	**D**	Least privilege is one of the most fundamental concepts used for controlling access to data. Whilst the others listed are valid, they are more indirect.	1.1
4	**B**	Availability is a concept that focuses almost exclusively on the delivery of a service. The other concepts relate to other security aspects or concepts.	1.2
5	**D**	Software audience and control set are specified by the Trustworthy Software Framework to ascertain which of the trustworthy levels (TL) is required. Software audience is based on market and need, which dictates the required control set.	1.3
6	**A**	Trustworthy Levels 1 and 2 are applicable to products with mass market, implicit need audiences, as defined under the Trustworthy Software Framework (TSF) Essentials specification and guidance documentation.	1.3
7	**A**	Security architecture is concerned with the parts of the system architecture that look at control, access and permissions. Enterprise architecture looks at how well the system meets business objectives.	2.1
8	**C**	Segmenting assets on a network by design will naturally minimise the severity of any compromise. Reducing the impact of compromise is one of the NCSC cyber security design principles. Establishing the context refers to asset inventories. Reducing disruption refers to availability threats and barriers to entry is not a design principle.	2.1
9	**D**	The five domains of the COBIT 5 processes are: • Evaluate, Direct and Monitor. • Align, Plan and Organise. • Build, Acquire and Implement. • Deliver, Service and Support. • Monitor, Evaluate and Assess.	2.2

Question	Answer	Explanation / Rationale	Syllabus Sections
10	**B**	SABSA is a methodology for developing business-driven security architectures at various levels that clearly support business objectives. It is vendor neutral and generic, but these are not the primary characteristic. The classifications listed relate to the Zachman model.	2.2
11	**C**	Guidance on basic installation and setup should always be sourced from the product vendor in the first instance. Additional information on hardening, patching and wider architecture concerns should be sourced from a reputable public body such as the NCSC.	2.3
12	**B**	NIST maintains the Cybersecurity Framework, a voluntarily adopted and widely used set of policy, guidance and implementation recommendations for organisations globally to assess and improve their security posture.	2.3
13	**A**	A security case is the best answer because it will outline the requirements needed to satisfy the declaration made, based on evidence and assessment. A security case may also contain common criteria or FIPS as part of its requirements.	3.1
14	**D**	As standalone pieces of technology, these are all considered technical controls, which are implemented as part of the wider security case to achieve security objectives and mitigate identified risks.	3.2
15	**A**	People and policy related items such as awareness training are considered to be organisational controls in the context of a security case. Where limitations in technical and other mitigating controls are identified, additional organisational controls can be deployed to mitigate residual risks.	3.2
16	**C**	A Security Case does not produce ‘results’ other than a decision, the Common Criteria and a Security Case are entirely different things, and there is no situation wherein a choice would be made between them. Common Criteria results may indeed be placed in Security Cases as evidence of assurance.	3.3
17	**A**	FIPS-140 is the official USA standard for approving systems utilising cryptographic elements for use in federal systems. It serves as the industry standard baseline specifically for cryptography, over less tailored frameworks such as Evaluation Assurance Levels (EAL).	3.3
18	**B**	Spoofing is the part of the STRIDE threat mnemonic that covers examples related to authentication and the impersonation of something or someone by an attacker. Masquerading means the same thing but is not part of STRIDE.	3.4

Question	Answer	Explanation / Rationale	Syllabus Sections
19	**B**	Poorly protected data-in-transit, such as clear-text network protocols like Telnet or HTTP, commonly disclose sensitive information to attackers, which is covered under the Information Disclosure threat category within the STRIDE model. Eavesdropping may involve capturing data, tampering with equipment or elevating privilege but they are secondary to the treat of information disclosure in this example.	3.4
20	**B**	During mergers and acquisitions, the most secure approach to integration, is to review the threat model of both systems and the impact of connecting them to uncover any additional threats or risks this may expose. Relying on historical accreditation or personal assurances could expose the parent company to new risks. Integration without any checks or reviews of the threat model is likely to expose both companies to extra risks.	3.5