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
21	**B**	Deployment of security controls manufactured by disparate vendors is an example of defence in depth. Reliance on a single vendor could present a security risk to an organisation if a vulnerability was exposed in their products.	1.1
22	**C**	A security control that defaults to a secure mode of operation following an unrecoverable failure is said to have failed securely. This prevents an attacker intentionally taking the control out of action in order to bypass or reduce its capability.	1.1
23	**A**	Resilience is the ability of a system to recover from errors quickly and completely.	1.2
24	**C**	Fail safe defaults are most closely related to the Trustworthy Software Framework (TSF) feature of security. “Ensure Error Handling is implemented comprehensively, and “fails safe and secure” [TE.07.30].”	1.2
25	**D**	The Trustworthy Software Framework (TSF) defines that Trustworthy Levels 1 and 2 are required to adopt the TS Essentials (TSE) control sets.	1.3
26	**D**	Enterprise Architects tend to operate at a higher, less focused level than Security Architects, and tend to have a broader, shallower scope.	2.1
27	**A**	An enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organisation. The intent of an enterprise architecture is to determine how an organisation can most effectively achieve its current and future objectives.	2.1
28	**D**	Attack surface reduction is the principle of only exposing the services and systems absolutely necessary to make initial compromise by an attacker significantly more difficult.	2.1
29	**A**	Framework, Process Descriptions, Control Objectives, Management Guidelines and Maturity Models are the five core components of the COBIT5 framework.	2.2

Question	Answer	Explanation / Rationale	Syllabus Sections
30	**B**	A coherent set of rules and templates, known as 'viewpoints' or ‘views’, including Strategic, Operational, Service Oriented and Technical views are features of the British Ministry of Defence Architecture Framework (MODAF)	2.2
31	**C**	The NCSC took over the administration of the CAPS program from GCHQ and helps organisations with Critical National Infrastructure (CNI) responsibilities to verify the cryptographic security of their products.	2.3
32	**A**	Security cases ensure that security is considered at all stages of the product or system lifecycle. A typical scenario of a security case not being used properly involves an organisation or system owner trying to retroactively fit security controls onto an already deployed system.	3.1
33	**C**	A security case is unconcerned with the operation of a consumer product, only the security aspects that impact upon it.	3.2
34	**B**	Staff Training is the only direct consequence of a significant change to a usage policy. The others may occur subsequently, but they are secondary effects. It is impossible to say if more security staff will be needed.	3.2
35	**A**	The business context section of a security case defines the reasons why the case is needed, how it will support wider business objectives and initiatives and who the key stakeholders are that are driving the requirements at an organisational level.	3.2
36	**D**	NCSC CAPS is an approved way for UK organisations to request NCSC evaluation and certification on the use of appropriate cryptographic algorithms specified within a system or products security case.	3.3
37	**D**	Denial of service is the part of the STRIDE threat mnemonic that covers examples related to availability or degradation of service.	3.4
38	**A**	The information disclosure part of the STRIDE mnemonic is concerned with protecting the confidentiality of information and preventing disclosure of said data to unauthorised parties.	3.4
39	**C**	Anti-virus evasion is a daily occurrence of modern cyber attacks and an organisation's threat modelling should take this into account and ensure that all security controls are regularly updated with the latest detection signatures and that they are regularly reviewed as fit-for-purpose against the threat model.	3.5

Question	Answer	Explanation / Rationale	Syllabus Sections
40	**C**	The threat model for an unsupported product must be updated to take into consideration the impact of any future vulnerabilities that could be released and the potential exposure factor based on the current security architecture. This will allow an organisation to either deploy mitigating controls or investigate replacing the control completely to avoid the risk.	3.5