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**	As this is human intervention Psychological acceptability is the only acceptable answer.	1.2
2	**A**	The governmental organisations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluation. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluation, version 3.1 Parts 1 through 3 (called "CC 3.1"), they hereby grant non-exclusive license to ISO/IEC to use CC 3.1 in the continued development/maintenance of the ISO/IEC 15408 international standard. source: http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf	3.1
3	**A**	A PP specifies generic security evaluation criteria to substantiate vendors' claims of a given family of information system products. Among others, it typically specifies the Evaluation Assurance Level (EAL)	3.1
4	**C**	http://csrc.nist.gov/publications/PubsSPs.html	2.3
5	**A**	An enterprise architecture (EA) is a conceptual blueprint that defines the structure and operation of an organization. The intent of an enterprise architecture is to determine how an organization can most effectively achieve its current and future objectives.	2.1
6	**A**	Specification of Security Targets security requirements, where a translation of the security objectives for the TOE into a standardised language is provided. source: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf page 65	3.1
7	**A**	Risk is the possibility of a negative or undesirable occurrence. There are two independent parts of risk: Impact and Likelihood. To reduce risk, one can reduce the impact, reduce the likelihood, or both. Risk can also be accepted (meaning that the full impact of the negative outcome will be borne by the entity at risk). The impact and likelihood of a risk are usually combined to create an estimate of its Severity. source: https://www.owasp.org/index.php/Glossary	4.1
8	**B**	The Trustworthy Software Framework (TSFr) is a collation of good practice, existing guidance and relevant standards across the five main facets of trustworthiness: Safety; Reliability; Availability; Resilience; and Security. source: http://tsfdn.org/ts-framework/	1.3

Question	Answer	Explanation / Rationale	Syllabus Sections
9	**A**	The NCSC was set up to help protect our critical services from cyber attacks, managing major incidents and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations. source: https://www.ncsc.gov.uk/about-us	2.3
10	**A**	source: https://www.ncsc.gov.uk/articles/become-cesg-approved-test-facility To carry out CPA and CC evaluations and CTAS and CAS assessments your company must: • get ISO 17025 accreditation against the Test Laboratory General Operational Requirements	3.1
11	**C**	Static packet filtering only looks at the incoming and outgoing packets, the other techniques look at additional factors such as applications, protocol non-compliance	4.4
12	**A**	Users are the biggest risk to security and ongoing education is needed to keep them aware of the threats.	4.3
13	**B**	Deming cycle is PLAN-DO-CHECK-ACT.	2.2
14	**A**	Security architecture looks at the parts of the system architecture that look at access and permissions. The Enterprise, management & Operational architectures look at process, structure etc.	2.1
15	**D**	These domains build on those present in COBIT 4.1 and align with other security standards such as those outlined in ITIL and ISO27000.	2.2
16	**B**	A vulnerability is something that can be exploited (e.g. lack of input validation) a threat is something that might occur e.g. a virus.	4.1
17	**A**	**Safety**: The ability of the software to operate without causing harm to anything or anyone. **Reliability**: The ability of the software to operate correctly. **Availability**: The ability of the software to operate when required. **Resilience**: The ability of the software to recover from errors quickly and completely. **Security**: The ability of the software to remain protected against the hazards posed by malware, hackers or accidental misuse. source: http://tsfdn.org/ts-framework/	1.3
18	**A**	The security case is looking at what the software does, not how it is coded. The evidence of the programmers training is relevant to check that they have the necessary security knowledge.	4.2

Question	Answer	Explanation / Rationale	Syllabus Sections
19	**B**	A & D are statements of fact, C a system can never be completely secure. Acceptably secure is a typical 'claim' of an overall system.	4.1
20	**A**	Aging and complexity of passwords provide a fail-safe (e.g. the passwords are rest) and safety in that they are complex. Least privilege is related to access, open design is related to resilience but at a design stage. Fail-safe is primarily related to safety.	1.4