Making IT good for society

BCS Level 4 Certificate in Governance, Organisation, Law, Regulation and Standards
Answer Key and Rationale QAN 603/0855/2

Question	Answer	Explanation / Rationale	Syllabus Sections
1	D	Storage capacity may have an impact on integrity, but it is more likely to be managed by service management or infrastructure planning.	1.1
2	B	The core entities supporting governance for an information security management framework are: - the Main Board; - the Risk Management Committee; - the Information Security Management Board.	1.2
3	A	This is the description of the term risk in respect to information security as stated in: https://en.wikipedia.org/wiki/Factor_analysis_of_information_risk	1.3
4	A	As stated in https://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257, security checkpoints built in to the project during several key processes will ensure progress toward the desired security end state at project closure.	1.4
5	C	ISO 27001 provides the foundation for multiple areas of compliance.	1.5
6	C	As stated in: NIST Special Publication 800-53 (Rev. 4) – Security Controls and Assessment Procedures for Federal Information Systems and Organisations – AC-6 LEAST PRIVILEGE - Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organisational mission/business needs.	2.1
7	C	Customers are external to the organisation and therefore not bound IT security policy.	3.1
8	D	Management and employees are the only options directly affected.	3.2
9	C	The Sarbanes-Oxley Act of 2002, sponsored by Paul Sarbanes and Michael Oxley, represented a huge change to federal securities law. It came as a result of the corporate financial scandals involving Enron, WorldCom and Global Crossing. Effective in 2006, all publicly-traded companies were required to implement and report internal accounting controls to the SEC for compliance	3.3

Question	Answer	Explanation / Rationale	Syllabus Sections
10	**A**	Under the GDPR, you must appoint a data protection officer (DPO) if you are a public authority (except for courts acting in their judicial capacity).	3.4
11	**A**	The main benefit from achieving the ISO/IEC 27001 lead auditor certification is the recognition that the individual can be engaged by certification bodies to perform information management system audits under their direction and management system.	4.1
12	**A**	CHECK is a penetration testing scheme as stated in: https://www.ncsc.gov.uk/articles/composition-check-team	4.2
13	**A**	All roles other than A are normally undertaken by external 3rd parties.	4.3
14	**B**	As stated in https://en.wikipedia.org/wiki/Regulation_of_Investigatory_Powers_Act_2000, the Defence Intelligence, GCHQ, HM Revenue and Customs, Secret Intelligence Service, Security Service and territorial police forces of Scotland are permitted to intercept a communication. Authorisation in the form of a warrant from Home Secretary or Cabinet Secretary for Justice is required.	5.1
15	**A**	As stated in https://www.iso.org/standard/54534.html, ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.	5.2
16	**A**	As stated in https://www.itgovernance.co.uk/blog/understanding-isoiec-270012013-and-its-required-documentation/, the Standard notes that 'the extent of documented information can differ from one organisation to another due to 1) the size of organisation and its type of activities, processes, products and services; 2) the complexity of processes and their interactions; and 3) the competence of persons.'	6.2

Question	Answer	Explanation / Rationale	Syllabus Sections
17	**A**	As stated in https://www.iso.org/certification.html, ISO are not involved in their certification, and do not issue certificates. External certification bodies perform this. As stated in https://www.iso.org/standard/54533.html, ISO/IEC 27002:2013 is designed to be used by organisations that intend to select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001.	6.3
18	**C**	As stated in https://www.iso.org/isoiec-27001-information-security.html, the ISO/IEC 27000 family of standards helps organisations keep information assets secure. Some organisations choose to implement the standard in order to benefit from the best practice it contains, while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed.	6.4
19	**D**	As stated in https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/, you only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals.	7.1
20	**B**	As stated in https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf, reporting of security breaches is the responsibility of the data controller.	7.2