BCS Level 4 Award in Risk Assessment
QAN 603/0866/7

Specimen Paper Answer Key

Version 3.0
July 2020

Change History

Any changes made to the specimen paper shall be clearly documented with a change history log. This shall include the latest version number, date of the amendment and changes made. The purpose is to identify quickly what changes have been made.

Version Number	Changes Made
Version 1.0 November 2016	Document created.
Version 2.0 September 2017	Updated following enhanced syllabus creation.
Version 2.1 July 2018	Updated – minor tweak
Version 3.0 July 2020	Major changes to questions to match updated syllabus (V3.0). Title page, change history table and related syllabus section added.

Related Syllabus

This specimen paper and answer key are related to the following syllabus:

BCS Level 4 Award in Risk Assessment Syllabus V3.0 March 2020

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	When assessing the impact of a risk, the associated productivity should be considered.	1.1
2	**D**	Blame is not one of the factors to be considered when conducting a risk assessment.	1.1
3	**A**	OCTAVE is the only recognised risk assessment methodology listed.	1.2
4	**B**	According to SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, risk assessments can be integrated into the risk management framework.	1.2
5	**C**	According to NCSC risk management guidance, when talking about systems it is essential to first state the function that you are trying to analyse.	1.3
6	**C**	As suggested in the NCSC risk management guidance, one size does not fit all. Organisations should establish the security risk management roles and decision-making processes that work for them (remembering that some organisations may have to comply with mandated requirements).	1.3
7	**A**	DDOS attacks are most successfully mitigated when the correct network defences are in place.	2.1
8	**C**	The accumulation of all of the stated vulnerability sources is indicative of a company with a weak security culture overall.	2.1
9	**D**	We are all human; we all make mistakes. A single silly mistake can be catastrophic.	2.2
10	**D**	Regular employee training is more effective than just training at induction. Refreshers and reminders are more likely to increase awareness and improve the culture.	2.3
11	**C**	If a mistake leads to a punishment, it is less likely the mistake will be reported. A key aspect of the cyber culture is then lost.	2.3
12	**B**	The salesperson although an individual is a company insider. An individual would be someone outside of the company. The salesperson has committed information theft.	2.4
13	**C**	A threat actor, also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organisation's security. Flood is a hazard or threat vector. An SQL injection attack is a threat vector. Failure to encrypt is a vulnerability.	2.4

Question	Answer	Explanation / Rationale	Syllabus Sections
14	**A**	The direction phase of the lifecycle is when goals for the threat intelligence program are set. This requires understanding which information assets and business processes need to be protected.	2.5
15	**A**	The correct order of stages for the intelligence lifecycle is Direction, Collection, Processing, Analysis, Dissemination, Feedback.	2.5
16	**B**	Complex solutions with in-demand skill sets normally have a high cost associated with them. In this situation managed services are most likely to be used to transfer the risk.	3.1
17	**B**	Cyber insurance is an example of treating risk by transferring it.	3.1
18	**D**	A risk owner should be knowledgeable about the risk, but must also have the authority to manage it within the business.	3.2
19	**B**	The Single Loss Expectancy (SLE) is used with the Annualised Rate of Occurrence (ARO) to calculate the Annualised Loss Expectancy (ALE). ALE = SLE x ARO	3.3
20	**C**	Quantitative methods are better suited to analysing potential costs - using such techniques as Annual Loss Expectancy (ALE). Qualitative methods may consider financial exposure, are usually quicker but tend to be subjective and 'broad-brush'. Neither is mandatory in all sectors.	3.3