Making IT good for society

BCS Level 4 Award in Risk Assessment
Answer Key and Rationale – QAN 603/0866/7

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**B**	ISO 27000 provides the definitions of generic terms related to information security.	1.1
2	**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. http://whatis.techtarget.com/definition/threat-actor	1.1
3	**A**	This question contrasts the concepts of 'appetite' and 'acceptance'. Appetite is a conscious decision to take on a maximum level of risk. Acceptance is a conscious decision to do nothing.	1.1
4	**B**	The Red Amber Green (RAG) colour scheme is almost universal in indicating severity - for risk as well as other measures.	1.4
5	**C**	Five steps defined in the syllabus as: 1 Identify assets. 2 Identify threats and vulnerabilities. 3 Assess the impact of threats and vulnerabilities on an organisation (assessment - not identification). 4 Identify ways to manage those threats and vulnerabilities (mitigation). 5 Monitor and report on risk management action.	1.2
6	**A**	ISO 27005 defines threat as: A potential cause of an incident, that may result in harm of systems and organization. A flood meets this definition.	2.1
7	**B**	ISO 27005 defines vulnerability as: A weakness of an asset or group of assets that can be exploited by one or more threats.	2.1
8	**B**	Benefits of using threat intelligence: Provides context and relevance to a tremendous amount of data; Empowers organisations to develop a proactive cybersecurity posture and bolster its overall risk management policies; Informs better decision making during and following the detection of a cyber intrusion; Drives momentum toward a cybersecurity posture that is predictive, not just reactive.	2.2

Question	Answer	Explanation / Rationale	Syllabus Sections
9	**D**	An attack vector is a path or means by which someone can gain access to a computer or network server in order to deliver a payload or malicious outcome. Spear Phishing typically uses Email as that path.	2.3
10	**A**	These terms are sometimes combined, but there is a distinct difference as set out in option A.	2.4
11	**C**	Whilst all potential answers have some substance, C provides the most logical of them all. Note that some methods may be a hybrid of two or more. If this is done, the hybrid has to be used consistently.	3.1
12	**A**	OCTAVE is qualitative. The NCSC website states that: "Octave Allegro is an asset-focussed method. The first step is establishing consistent, qualitative risk measurement criteria specific to the organisation's drivers and objectives." https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks.	3.2
13	**B**	COBIT was developed by ISACA - and the organisation retains the copyright.	3.1
14	**D**	A B and C are not true. The method is still usable but is unsupported. NCSC website https://www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks.	3.3
15	**B**	Answer 'b) Data Protection' is irrelevant to the question. Typical choice factors are: The overall cost of using the method; The scope of the project; Ensuring the required resources are proportionate and sustainable; Any commercial aspects that could restrict its use; Can we use the method at any time, on any system, using any resources? Are there any licencing restrictions?	3.4
16	**A**	"It is known as a "zero-day" because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate its actions" - Wikipedia - Zero-day (computing).	4.2
17	**B**	Insurance is the chief means of risk transference - one transfers the risk to an insurance company in return for cash - or premium	4.3

Question	Answer	Explanation / Rationale	Syllabus Sections
18	**A**	The SIRO is defined in ISO 27000 as the 'Person or entity with the accountability and authority to manage a risk'.	4.4
19	**C**	Quantitative methods tend to be complex, have no standards and often require special tools. Qualitative methods are supported by many standards and often do not require any tools. They are, however, subjective, and the quality of the results depends heavily on the quality of the participants.	4.1
20	**B**	Vulnerability research often involves deliberate attempts to overcome security controls. The outcome of this is often perceived negatively, as the knowledge gained can be exploited for illegal gain. It can also provide invaluable insights. The methods used echo those used by illicit intruders, and are thus tainted and some consider to be unethical.	4.2