

BCS Level 4 Certificate in Information and Cyber Security Foundations
Answer Key and Rationale – QAN 603/3214/1

Question	Answer	Explanation / Rationale	Syllabus Sections
1	A	These can be traced back to origin. Texts may not be reliable.	3.8
2	C	This is the organisation that researches vulnerabilities. SANS and ISC2 are training organisations.	2.5
3	A	Security policies are part of a company complying with legislation such as GDPR.	1.1
4	C	Changing the passwords is an attempt to contain the incident.	6.3
5	D	All these can be highlighted through auditing. User training will not be highlighted through auditing.	3.10
6	A	Cisco identifies several signature types. Atomic is a single activity or event. String and multi-string refer to pattern matching.	7.4
7	B	Business Impact Analysis and Threat and Risk Analysis are both part of the impact analysis stage of standard ISO 22301.	5.3
8	C	This type of attack exploits vulnerabilities in web browsers.	7.1
9	C	By carrying out risk assessments organisations can adopt rational security policies.	2.1
10	B	A user can deny involvement in a breach.	2.4
11	B	This is the industry standard. Security design is constantly evolving.	4.2
12	C	COBIT and Risk IT were published by Information Systems Audit and Control Association.	3.11
13	A	This definition is a quote from www.itgovernance.co.uk	3.3
14	A	Redundancy is part of business continuity management but not incident response.	5.2
15	C	Poor security management leaves intellectual property vulnerable.	2.6
16	A	This is the definition of security architecture taken from Techopedia.	4.1
17	A	Tests should be carried out at regular intervals and after system changes.	2.9
18	D	These 3 are all part of Risk IT. c is part of COBIT.	3.5
19	B	The infected systems in a botnet are called zombies.	6.1
20	B	This is a targeted phishing attack.	6.2