BCS Level 4 Award in Business Processes
Answer Key and Rationale – QAN 603/3215/3

| Question | Answer | Explanation / Rationale | Syllabus Sections |
|---|---|---|---|
| **1** | C | For all criminal activities the police are the initial external agency that should be liaised with. | 2.1 |
| **2** | A | Faraday bags stops external signals thus preserving evidence prior to analysis or a remote signal for data to be wiped. | 2.3 |
| **3** | B | Home Office Guidance – Evidence in criminal investigations – version 3.0 based on the Police and Criminal Evidence Act 1984, Criminal Procedure and Investigations Act 1996, Criminal Justice Act 2003 and Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material (2011). | 2.3 |
| **4** | B | The feedback loop process part of incident response from SANS / NIST links to a similar process in ITIL, via the Deming process. | 1.1 |
| **5** | D | Setting out a cyber incident response as a starting point to reduce risk and defend key assets is most closely aligned with the service strategy aspect of ITIL. | 1.1 |
| **6** | B | The criminal could initially be prosecuted under Section 2 of the Act - unauthorised access with intent to commit or facilitate commission of further offences. | 2.1 |
| **7** | A | Complete the feedback loop of updating prepared phase of the six stages of incident response. | 2.2 |
| **8** | C | A threat analysis should be completed as part of the preparation stage of the overall cyber security program i.e. ISO 27001 and integrated into the CIMP. | 2.2 |
| **9** | D | As defined as step one by the UK National Cyber Security Centre and GCHQ - Establish an incident response capability: Identify the funding and resources to develop, deliver and maintain an organisation-wide incident management capability. | 2.2 |
| **10** | A | Building up people, process, training and response process is part of designing how the response will be done using documents and best practice. Therefore, the nearest mapping in ITIL is service design. | 1.1 |
| **11** | B | 72 hours as defined in Article 35 GDPR. | 2.1 |
| **12** | D | Article 35 GDPR refers to regulatory authority which is the Information Commissioner's Office (ICO). | 2.1 |
| **13** | B | ACPO - To comply with principle 3, records must be kept of all actions taken in relation to digital evidence, which could include photographs / diagrams of equipment locations, details of any information provided by persons present, and records of any actions taken at the scene. | 2.3 |
| **14** | D | Communicating lessons learnt and updating processes and controls are all elements of the follow-up phase of cyber incident management. | 2.2 |
| **15** | A | The use of penetration testers in Red Teams as external hackers allows CIRTs to update responses and improve plans. | 2.2 |

| Question | Answer | Explanation / Rationale | Syllabus Sections |
|---|---|---|---|
| **16** | B | Recovery is a key stage to ensure all data is clean along with traces of any malware, rootkits, remote access Trojans etc. that could still be in the system. Therefore, recovering to a known point before the attack reduces the risk of a hacker maintaining access. | 2.2 |
| **17** | D | Without a write-blocker defense would argue that the disk has been 'written to' during the collection process contaminating the evidence. | 2.3 |
| **18** | A | ITIL feedback loop process for improvement in the same way the incident response cycle has a lesson learnt part to improve the prepare phase. | 1.1 |
| **19** | A | For any terrorist-based information the police must be contacted. | 1.2 |
| **20** | B | CISO is defining the initial part of a concept or strategy of the Incident Response Service. | 1.1 |