Making IT
good for
society

BCS Level 4 Certificate in Cyber Security Introduction
Answer Key and Rationale QAN 603/0830/8

Question	Answer	Explanation / Rationale	Syllabus Sections
1	**A**	A directive control requires the user to do something in a particular way. This might be the order in which Two Factor Authentication (TFA) takes place. Stopping the user doing something wrong is a preventative control. Correcting an erroneous entry by a user is a corrective control. Identifying a user has done something wrong is a detective control.	7.1
2	**A**	Fast flux introduces numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. Whereas in IP spoofing, a cracker masquerades as a trusted host to conceal his identity, spoof a Web site. In a DDoS attack multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack.	6.1
3	**A**	Ransomware requires a system to be infected through a crypto virology attack. This is usually delivered through an attachment to an email. If the delivery email looks genuine, then clicking on the attachment to open it encrypts the victim's files. An attacker can also exploit poorly configured firewall to launch a ransomware attack. Disrupting power supply will affect the server backups but will not facilitate a ransomware attack.	6.1
4	**B**	CIA is a widely-applicable security model standing for Confidentiality, Integrity and Availability. This principle is applicable across the whole subject of Security. If any one of the three are breached it will have serious consequences.	2.1
5	**B**	In SSL v2.0, a man-in-the-middle can intercept the client message specifying the set of suites supported, and remove from it all strong suites. If both the server and client support the same weak suite, then the agreement will succeed with some weak suite being chosen. In SSL v3.0, this is not possible, because the protocol later uses the negotiated authentication key to belatedly verify the contents of all messages sent during the session establishment dialogue.	6.1

Question	Answer	Explanation / Rationale	Syllabus Sections
6	**A**	Security audits constitute 'detective control' where auditors *detect* some anomaly during the audit trails. Preventive controls include security guard such as antivirus, etc. Networked control is closed loop through a communication network; and financial control is the control of accounts.	7.1
7	**B**	Attack chain involves 7 activities in this order: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & control, Actions on objective.	7.1
8	**B**	Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. It is therefore important to validate the user by checking a shared secret. HTTPS does nothing to defend against CSRF; and likewise firewalls and other network configurations could not protect from CSRF.	5.1
9	**C**	Anti-virus software is a protective control. Procedural controls are things like policies. Deterrence is something that discourages wrong doing.	7.1
10	**A**	Open ports will increase the attack surface and result in introducing a vulnerability of bypassing security controls of a protected system. This will increase the overall operational costs including the burden of additional workload on the staff. Because of the accidental nature, there may not be any formal remedies until this vulnerability is discovered (e.g. through periodic scanning of the ports). Physical protection has no direct relevance with the open ports.	5.1
11	**A**	Horizon scanning is a process which uses the idea of looking as far ahead as possible to look for trends, developments, research and related areas to help predict what threats we might face in the future. The OECD definition of horizon scanning is "a technique for detecting early signs of potentially important developments through a systematic examination of potential threats and opportunities, with emphasis on new technology and its effects on the issue at hand." http://www.oecd.org/site/schoolingfortomorrowknowledgebase/futuresthinking/overviewofmethodologies.htm	9.1

Question	Answer	Explanation / Rationale	Syllabus Sections
12	**D**	As an example, CCTV (whilst a technical solution) is a physical control, used for detecting unauthorised access. An acceptable use policy is a procedural control. Locks on doors are physical controls, even if the locks are electric. User logon password requirements are a technical control.	7.1
13	**C**	A router is designed to look at the address in a data packet and send it on to the appropriate part of a network to reach that address. A firewall is designed to limit the traffic coming into an organisation's IT systems and to protect from attackers. A DMZ is a zone designed to add an additional layer of security to an organization's local area network by "hiding" the internal network from the Internet or another network. A hub is a link between different networks or individual computers.	5.1
14	**A**	Accidental deletion of data is generally caused by human error. The other options require a secure physical location to ensure data protection and its availability.	6.4
15	**B**	If all software is installed on the terminal, it is a thick client and this will require significant processing power in the terminal. Thin client is a terminal connected to a server network, where the device itself has very limited/ no processing power, nor software installed. There is no link to the ability of the users. The use of web-based software is called smart client and although there may not be much processing power in the terminal, it must have some.	5.2
16	**A**	Security objectives remain the same when the threats landscape is changed. However, the security requirements are directly related to the threats paradigm. There could be changes in the budgetary requirements to meet the new security requirements and also some changes in the security policy to reflect the changes.	4.1
17	**D**	The amount of data transferred is likely to be small from smart phones and similar devices. However, the other options are realistic risks that organisations allowing staff to utilise BYOD need to consider very carefully.	10.1
18	**B**	Business should drive security controls so as to ensure alignment of security objectives with the business objectives. Costs and review needs depend on the business needs.	4.2

Question	Answer	Explanation / Rationale	Syllabus Sections
19	**A**	Intrinsic assurance is the security quality and rigour provided by the developer of the system. It does not cover independent security evaluation and testing (such as in the Extrinsic assurance) and therefore it could not be evaluated by existing security evaluation criteria such as Common Criteria. Parameters of implementation and operational assurances can be evaluated by external auditors.	3.2
20	**A**	Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments. Common Criteria is more formally called 'Common Criteria for Information Technology Security Evaluation'.	8.3
21	**B**	This is a legal requirement for the companies operating in the UK to inform the ICO of any breach of personal data. They must also notify customers if the breach is likely to adversely affect customers' privacy, and keep a breach log.	1.2
22	**C**	A cyber-attack may impact a business in a number of ways including financial and social (reputational) losses and legal actions brought by the affecters. However, there will be no considerable difference in the use of office supplies.	1.3
23	**B**	Darknets cannot be accessed through standard web browsers. Whereas a surface web is visible and is indexed by typical search engines (such as Google or Bing). Tor is a privacy-aware software to ensure anonymous communications. Unallocated space or clusters is the hard disk storage space that is not assigned to any drive.	2.4

Question	Answer	Explanation / Rationale	Syllabus Sections
24	**D**	A risk register is a risk management tool. It has a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures. Whereas, Mind map is a diagram in which information is represented visually, usually with a central idea placed in the middle and associated ideas arranged around it; and the Capability Maturity Model (CMM) is a methodology used to develop and refine an organisation's software development process. A Certified Risk Analyst (CRA) is a risk management professional designation offered by the Academy of Finance & Management.	2.3
25	**C**	The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.	2.5
26	**A**	Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.	3.1
27	**D**	Security vulnerabilities are usually introduced through poor configuration or inadequate patching policies or processes. Penetration testing is the process to identify these security vulnerabilities with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.	3.4
28	**A**	A threat intelligence feed is an ongoing stream of data related to potential or current threats to an organization's security. Threat intelligence feeds are third-party streams of indicators or artefacts, with the singular goal of learning from other organizations' access and visibility to improve your own threat awareness and response.	3.5
29	**A**	Security is not something that can be a bolt-on to a system. It has to be woven in the fabric of the system. The best way to do it is to consider security during all of the system development phases starting from the requirements gathering phase.	4.1
30	**B**	Security requirements are generally driven by the security objectives of a product/system. Security context / environment and threats analysis are also fed in the elicitation of security requirements. On the basis of security requirements, security functions are identified, security solutions are chosen, and security guidelines are prepared.	4.4

Question	Answer	Explanation / Rationale	Syllabus Sections
31	**D**	WiFi Protected Access (WPA) is a security standard for computing devices equipped with WiFi. It improved upon and replaced the original WiFi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP, and it also provides user authentication - WEP's user authentication was considered insufficient.	5.1
32	**B**	Star networks are one of the most common computer network topologies. In its simplest form, a star network consists of one central hub which acts as a conduit to transmit messages. In star topology, every node (computer workstation or any other peripheral) is connected to a central hub. The switch is the server and the peripherals are the clients.	5.2
33	**A**	Humans are frequently considered as the weakest link in any organisation's cyber security chain.	6.2
34	**A**	Advances in the technology landscape are introducing new paradigms that may contain vulnerabilities, but they may not be exploited with the classical attack techniques. Changes might have been made to overcome the previous gaps but may contain some other vulnerability that needs to be exploited. Likewise, increasing numbers of internet-enabled devices require new attack techniques to cope with the resilience offered by this paradigm, with the possibility of remote detection and remediation of any traditional attack. However, if an old system is not patched, or a password is weak, then any of the classical attack techniques could be employed by a malicious entity to attack the system.	6.3
35	**C**	Businesses can implement security solutions within their perimeter to improve the state of security for their resources. Endpoint products do not provide any considerable protection from the insider threats. Likewise, corporate insurance has no such requirement either. The prices of these solutions vary and depend on a number of other parameters.	7.1
36	**D**	Contract law consists of a large body of rules and guidelines that address contract formation and enforcement. When a party (a company in this question) fails to deliver the agreed service to the other party (customers in this question) than the most relevant legislation is the contract law.	8.2

Question	Answer	Explanation / Rationale	Syllabus Sections
37	**A**	25 May 2018 is the date set by the European Commission.	8.4
38	**B**	All professional bodies have a set of professional ethics rules that apply to all of their members.	8.5
39	**A**	Reliability of a publication is measured through the quality of evaluation process used by the publisher. Conference proceedings, journals and whitepapers are peer-reviewed by the experts of their respective fields who evaluate the quality of the work presented in the manuscript. Whereas, open and unmoderated avenues such as online chat forums have no control over the quality of the contents being shared over there.	9.2
40	**C**	Trend analysis is based on the idea that what has happened in the past gives an idea of what will happen in the future. Therefore, a risk manager can use trend analysis to predict the future events based on past data.	10.2