Making IT good for society

BCS Level 4 Award in Business Processes
QAN 603/3215/3

Specimen Paper A

Record your surname / last / family name and initials on the answer sheet.

Sample paper only 20 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

A number of possible answers are given for each question, indicated by either **A. B. C. or D**. Your answers should be clearly indicated on the answer sheet.

Pass mark is 13/20.

This qualification is regulated by Ofqual (in England).

1 An analyst is developing new incident management processes for liaising with external agencies. Who **SHOULD** be the initial agency for criminal matters?

A Company lawyer.
B Criminal Prosecution Service.
C Police.
D Data protection officer.

2 An analyst needs to secure an infected tablet computer from the corporate wireless network and 4G mobile data for forensic analysis and to preserve evidence. How can this be done?

A Put it in a Faraday bag.
B Put it in a plastic evidence bag.
C Disable Wi-Fi and data services.
D Do a factory reset and turn it off.

3 As part of an intrusion investigation a team is collecting images and log files taken from devices. What must be done to ensure evidence is handled correctly between people?

A Copy the data onto a common full access shared drive.
B Maintain a chain of evidence.
C Use branded hard disks for storing information.
D Modify every file name captured with each person's name.

4 Where is the lessons learnt aspect of a cyber incident management program **MOST LIKELY** to fit into the ITIL processes?

A Asset management.
B Continuous service development.
C Service desk.
D Application management.

5 An analyst is creating a cyber incident response capability to reduce risk and defend key assets such as networks, data and applications. Where would this process **BEST** map to in ITIL?

A Application management.
B Change control.
C Capacity management.
D Service strategy.

6 An analyst discovers three of their cloud servers have been attacked and are now bots of a larger criminal botnet but not activated. What initial law **COULD** the cybercriminal be prosecuted under?

A Communications Act (2003).
B Computer Misuse Act (1990).
C GDPR.
D Fraud Act (2006).

7 After a cyber security incident, what must happen to information, controls and processes?

A Update with lessons learnt about the attack.
B Do nothing with them.
C Archive them as there will not be another attack.
D Delete information due to GDPR.

8 Where does threat analysis fall within the cyber incident management process?

A Regulation.
B Delivery.
C Preparation.
D Investigation.

9 In incident response process management, what is the **first** stage an organisation must complete?

A GDPR.
B Report.
C Recover.
D Prepare.

10 Incident response management needs an initial preparation phase with policies and key tools. Where in ITIL would this **MOST LIKELY** align?

A Service design.
B Service level agreements.
C Syslog monitoring.
D Technical management.

11 An analyst discovers a data breach in their organisation. According to GDPR, in what period of time must the breach be reported?

A 36 hours.
B 72 hours.
C 1 month.
D It is not reportable.

12 Which organisation controls breach reporting?

A NCSC.
B GCHQ.
C NCA.
D ICO.

13 In a data security breach investigation an analyst discovers a small Linux computer plugged directly into the company network. What is the first step in collection of evidence?

A Disconnect the device from the network.
B Photo and document the device and physical connections.
C Remove any storage for forensic investigation.
D Disable main gateway routers for the enterprise.

14 A Cyber Incident Response Team (CIRT) has just recovered from a small data breach involving three company laptops used by sales people. An investigation shows that disk encryption would have stopped this, and recommendations are made to senior managers. In which phase of the incident management process are the team?

A Kill-chain.
B Recover.
C Eradication.
D Follow-up.

15 A Cyber Incident Response Team (CIRT) has finished the preparation phase for their organisation. How **COULD** the organisation test their state of readiness?

A Red team simulated attack.
B Blue team simulated attack.
C Disable the firewalls.
D Do nothing, an attack will never happen.

16 As part of an incident, malware was discovered then isolated on two servers. The infected disks were destroyed and replaced with new clean disks. The next step is to copy files from backups 24 hours before the incident. What phase of the incident management process is happening?

A Contain.
B Recover.
C Communicate.
D Test.

17 An analyst is investigating an incident on a laptop and collects a disk image for forensic analysis by the authorities, they fail to use a write-blocker. How **COULD** this affect the evidence?

A It would stop the USB ports on the laptop being used for collecting evidence.
B A write-blocker would strip out all the infected files being investigated.
C All the files are in a different format to the original file system.
D It would be impossible to prove evidence has not been modified during collection.

18 ITIL has a theme of constant improvement, how would this relate to cyber incident response process?

A Corrective action plan.
B Eradicate attackers.
C Prepare policy documents.
D Recover data.

19 During a regular restore test of file servers in an organisation, an analyst discovers pictures and documents relating to terrorism. Who would be the **PRIMARY** agency to contact?

A Police.
B MI5.
C GCHQ.
D ICO.

20 A CISO has told their board of directors about a concept for improving cyber security response to incidents, to help protect the organisation. What phase of ITIL is the CISO considering?

A Business continuity.
B Service strategy.
C Disaster recovery.
D Service transition.

-End of Paper-