Making IT
good for
society

BCS Level 4 Certificate in Information and Cyber Security Foundations
QAN 603/3214/1

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.

Copying of this paper is expressly forbidden without the direct approval of BCS, The Chartered Institute for IT.

This qualification is regulated by Ofqual (in England).

Copyright © BCS 2018

1 Which of these **SHOULD** be used to increase security awareness?

a) Webinars.
b) Newsletters.
c) Blogs.
d) Texts.

A a, b and c only.
B a, b and d only.
C b, c and d only.
D a, c and d only.

2 Which of these is a recognised industry source of information on security threats and vulnerabilities?

A SANS.
B ISC2.
C Secunia.
D CERT.

3 Why is cyber security important for SMEs?

A It helps them to ensure that they are compliant with the local legal and regulatory framework.
B It isn't important as SMEs are not subject to the same legal and regulatory framework as large enterprises.
C Without it, large enterprises would be able to take advantage of SMEs.
D It helps them to gain business advantage over large enterprises.

4 An incident is suspected, and in response system administrator passwords are changed. This is an example of which type of response?

A Legal.
B Eradication.
C Containment.
D Exploitation.

Copyright © BCS 2018

5 Which of these are reasons to carry out security auditing?

a) Improved patch management.
b) Improved user training.
c) Improved hardware configuration.
d) Improved software configuration.

A a, b and c only.
B b, c and d only.
C a, b and d only.
D a, c and d only.

6 Which type of signature identifies a sequence of actions distributed across multiple hosts?

A Composite.
B Atomic.
C String.
D Multi-string.

7 Which of these are part of the impact analysis stage of the business continuity management lifecycle?

a) BIA.
b) CIA.
c) TRA.
d) NSA.

A a and b only.
B a and c only.
C b and c only.
D b and d only.

8 Client-side scripts are injected into web pages viewed by other users. What type of attack is this?

A SQLi.
B MitM.
C XSS.
D DoS.

Copyright © BCS 2018

9 Risk assessment allows an organisation to do which of the following?

A Cut costs.
B Cut staff.
C Increase security.
D Increase staff.

10 An analyst cannot track a user's use of an application. What does this allow?

A Discoverability.
B Repudiation.
C Vulnerability.
D Escalation.

11 At which point in the design process **SHOULD** security architecture interact with enterprise architecture?

A Once the enterprise architecture has been decided.
B It is a continual process to be reviewed constantly.
C Only during the initial design phase.
D During the risk assessment stage.

12 Which organisation published Risk IT and COBIT?

A BCS.
B BSI.
C ISACA.
D ISSA.

13 'A centrally managed framework for keeping an organisation's information safe.' What does this describe?

A An information security management system.
B A software development management system.
C A network management system.
D A firewall management system.

Copyright © BCS 2018

14 Which of these relate to incident response and business continuity management?

a) Identification.
b) Containment.
c) Recovery.
d) Redundancy.

A a, b and c only.
B a, b and d only.
C b, c and d only.
D a, c and d only.

15 Which of these is a likely result of poor security management?

A Improved corporate reputation.
B Improved revenues.
C Damaged intellectual property.
D Reduced staffing levels.

16 Which of these defines security architecture?

A A design that addresses the needs and potential risk of a particular environment.
B A universally applicable design that addresses needs and potential risks.
C A design that states the needs of an environment.
D A design controlled by user acceptance and requirements.

17 When **SHOULD** penetration testing be carried out?

A After system changes have been made.
B Before hardware is decommissioned.
C After a security audit had been completed.
D During system changes.

Copyright © BCS 2018

18 Which of the following are principles of the Risk IT methodology?

a) Align the IT risk management with ERM.
b) Balance the costs and benefits of IT risk management.
c) Assess maturity and capability per process and help to address gaps.
d) Promote fair and open communication of IT risks.

A a, b and c only.
B b, c and d only.
C a, c and d only.
D a, b and d only.

19 A botnet is a network of what type of systems?

A Handler.
B Zombie.
C Legacy.
D Phone.

20 Which of these is a characteristic of a targeted attack?

A Spam email.
B Spear phishing.
C Worm.
D Network sniffing.

-End of Paper-

Copyright © BCS 2018