Making IT good for society

BCS Level 4 Award in Risk Assessment
QAN 603/0830/8

Specimen Paper A

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

Specimen 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.

This qualification is regulated by Ofqual (in England).

1 Which role is defined as the 'person or entity with the accountability and authority to manage a risk'?

A Risk manager.
B Risk owner.
C Risk assessor.
D Risk analyst.

2 Which of the following is a 'threat actor'?

A Flood.
B SQL injection.
C Disgruntled insider.
D Failure to encrypt.

3 What risk management term **COULD** be described as ‘the overall amount of risk judged appropriate for an organisation to tolerate, agreed at board level’?

A Risk appetite.
B Risk index.
C Residual risk.
D Risk acceptance.

4 Which might indicate the relative severity of a risk?

A Timeline.
B RAG status.
C Dependency model.
D Financial statement.

5 Which is **NOT one** of the five steps of risk management?

A Asset identification.
B Threat and vulnerability identification.
C Impact identification.
D Risk mitigation.

6 What is a flood?

A Threat.
B Vulnerability.
C Exploit.
D Impact.

7 What is 'a weakness of an asset or group of assets that can be exploited by one or more threats'?

A Attack.
B Vulnerability.
C Impact.
D Exploit.

8 What is the **PRIMARY** benefit of using threat intelligence?

A It provides positive attribution against attackers.
B It permits a proactive approach to managing information risk.
C It provides access to government intelligence resources.
D It removes the need for risk analysis.

9 Which attack vector is **MOST** commonly used to deliver a spear phishing attack?

A SQL injection.
B USB memory stick.
C Web browser.
D Email.

10 What is the difference between a vulnerability assessment and a penetration test?

A A vulnerability assessment looks for known vulnerabilities - a penetration test exploits found vulnerabilities.
B There is no difference.
C A vulnerability assessment is a desktop exercise - a penetration test operates on the live environment.
D A vulnerability assessment is performed during working hours - a penetration test at night.

11 Which is the **BEST** reason for using a single risk assessment method?

A Licensing costs are reduced.
B Skills requirement is limited.
C Results are comparable across the organisation.
D Results form a convenient shorthand.

12 What term **BEST** describes the OCTAVE risk assessment method?

A Qualitative.
B Quantitative.
C Quotient assessment.
D Quality assurance.

13 From which organisation does the COBIT risk management framework originate?

A Information Security Forum (ISF).
B ISACA.
C NIST.
D NICSC.

14 What is the **MAIN** disadvantage of using the CESG Information Assurance Standard 1 and 2 risk methodology?

A The tool will not run on MS Windows versions later than XP.
B All practitioners must be security cleared to DV.
C The methodology is only available to HMG departments.
D The method and supporting tool is no longer supported.

15 Which of the following are taken into account when choosing a risk assessment methodology?

a) Cost.
b) Data protection.
c) Commercial restrictions.
d) Skill requirements.

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

16 What is a zero-day vulnerability?

A An undisclosed vulnerability that can exploited before mitigations are developed.
B A vulnerability that is attacked 'zero-days' after MS 'patch Tuesday'.
C A vulnerability that is exploited by rapidly developed malware - that takes 'zero-days' to implement.
D A legacy vulnerability that has never been exploited - until now.

17 Which is an example of risk transference?

A Installing firewalls.
B Buying insurance.
C Outsourcing infrastructure.
D Analysing control gaps.

18 Who is **NORMALLY** responsible for decisions relating to the management of a specific information security risk?

A The Senior Information Risk Owner (SIRO).
B The Data Protection Officer (DPO).
C The Information Asset Owner (IAO).
D The Chief Information Security Officer (CISO).

19 Which of the following is a **MAJOR** disadvantage of a qualitative risk assessment method?

A Complexity.
B Lack of standards.
C Subjectivity.
D Requires special tools.

20 What is the **MOST** significant barrier to using vulnerability research methods?

A Expense.
B Ethics.
C Time.
D Quality.

-End of Paper-