BCS Level 4 Certificate in Security Case Development and Design Good Practice QAN 603/0904/0

Specimen Paper

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 for 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.

The pass mark is 13/20.

This is a specimen examination paper only.

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).
1. A network administrator notices that some users are turning off or otherwise bypassing a software security system. Which of the core IT Security Design Principles has been violated to cause this?
   A. Psychological acceptability.
   B. Open design.
   C. Fail-safe defaults.
   D. Economy of mechanism.

2. Which of the following is a **PRIMARY** principle when designing a secure system?
   A. To know what the most current technology available is.
   B. To understand what is being protected.
   C. To know what technology is being used.
   D. To understand the impact of the system being compromised.

3. The Evaluation Assurance Level (EAL) of an information security product is specified in which of the following documents?
   A. The Protection Profile.
   B. The Target of Evaluation.
   C. The Rainbow Series.
   D. ISO/IEC 27001.

4. SP 800 Computer Security is a publication series by which national body?
   A. CESG.
   B. NCSC.
   C. NIST.
   D. GCHQ.
5 Which of the following BEST describes where the boundary between enterprise architecture and security architecture may be defined?

A Enterprise architects design, build and oversee the implementation of computer and network security, whereas security architects are concerned with business practices and policies.

B Security architects are business-driven and focus upon risk and opportunity, whereas enterprise architects focus on operational and technical requirements related to business policy.

C Security architects focus on operational and technical requirements related to business policy, whereas enterprise architects are business-driven and focus upon configuration and testing.

D Enterprise architects are concerned with business practices and policies, whereas security architects design, build and oversee the implementation of computer and network security.

6 Which of the following is a description of enterprise architecture?

A It focuses on business processes and objectives.

B It includes technologies and specific products.

C It shows the locations of necessary security controls.

D It describes the implementation of computer security.

7 Which approach to guidance does NCSC employ in its publications to the public?

A Advice.

B Standards.

C Policy.

D Legislation.

8 When seeking Common Criteria certification, which document describes the security properties of a Target of Evaluation (TOE) and may claim that it conforms with a particular Protection Profile?

A Security Target (ST).

B Security Case (SC).

C Evaluation Assurance Level (EAL).

D Security Functional Requirements (SFRs).
9. The ability of a system to deliver the requested service is related to which of the following?

A. Resilience.
B. Availability.
C. Safety.
D. Security.

10. Which of the following is **NOT** a feature of trustworthiness, as defined by the Trustworthy Software Foundation (TSFdn)?

A. Reliability.
B. Integrity.
C. Resilience.
D. Security.

11. Which of the following core IT security design principles **CANNOT** be applied to the root account of a UNIX operating system?

A. Least privilege.
B. Defence in depth.
C. Open design.
D. Separation of privileges.

12. Which of the following is unlikely to be considered by a security case?

A. People.
B. Processes.
C. Technology.
D. Manufacturer.

13. Which of the following practise is **BEST** suited to meeting evolving cyber threats?

A. Changes in system configurations to include system hardening.
B. An automatic feedback loop for constant learning and improvement.
C. Upgrades in software within the vendor recommended timeframes.
D. Availability of anti-malware products.
14. As part of the common criteria evaluation the TOE is evaluated against which of the following?

A. Evaluation assurance levels.
B. Security assurance requirements.
C. Security functional requirements.
D. Security targets.

15. Which of the following would NOT be likely to appear in the security case for a consumer product?

A. The potential impact of a successful attack.
B. The potential severity of a successful attack.
C. The operation of the consumer product.
D. Known threats against similar systems.

16. Which of the following will future-proof the internal security of a network?

A. Ongoing user education.
B. Buying a newer firewall.
C. Upgrading network cabling.
D. Enforcing strong passwords.

17. ITIL implemented a never-ending cycle of improvements by incorporating the Deming cycle. Which of the following is NOT part of this approach?

A. Act.
B. Observe.
C. Plan.
D. Check.

18. Which aspect of system testing does NOT need to appear as evidence in a security case?

A. Expected test results.
B. Chosen test plan.
C. Outcome of the tests.
D. Test choice justification.
19 Which of the following TSFdn features is **MOST** related to fail-safe defaults?

A Reliability.
B Resilience.
C Security.
D Safety.

20 As system security increases, which of the following are likely to be targets for attack?

a) OS features.
b) Applications.
c) User access points.
d) Mobile devices.

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

-End of Paper-