Making IT
good for society

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

## 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 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.

This is a specimen examination paper only.



**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 **one** 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 international standard for computer security certification does the Common Criteria for Information Technology Security Evaluation adhere to?

**A** ISO/IEC 15408.
**B** ISO/IEC 27000.
**C** ISO/IEC 27001.
**D** ISO/IEC 26262.

**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 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.

**6** 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).

**7** OWASP classifies risk as the product of which **two** of the following factors?

**A** Likelihood and impact.
**B** Likelihood and threat.
**C** Impact and vulnerability.
**D** Vulnerability and likelihood.

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

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

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

**A** Advice.
**B** Standards.
**C** Policy.
**D** Legislation.

**10** Which security standard must all Common Criteria testing laboratories comply with?

**A** ISO/IEC 17025.
**B** ISO/IEC 15408.
**C** ISO/IEC 27001.
**D** NIST SP 800-160.

**11** As computer security threats have evolved over time, perimeter protection devices have been developed to keep abreast of this evolution. Which of the following technologies provides the weakest level of protection for a network?

**A** Application proxy firewalls.
**B** Stateful packet filtering.
**C** Static packet filtering.
**D** Deep packet inspection.

**12** 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.

**13** ISO/IEC 27001 incorporated the Deming cycle. Which of the following is **NOT** part of this approach to security?

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

**14** A document that describes an organisation's logical zones, e.g. internet zone, external DMZ and management zone, would be associated with which **one** of the following?

**A** Security architecture.
**B** Enterprise architecture.
**C** Management architecture.
**D** Operational architecture.

**15** COBIT 5 processes are split into 5 domains. Which **one** of the these is **NOT** one of the domains?

**A** Align, Plan and Organise.
**B** Build, Acquire and Implement.
**C** Monitor, Evaluate and Assess.
**D** Build, Monitor and Support.

**16** Which **one** of the following is a system vulnerability rather than a threat?

**A** Peer-to-peer file sharing of executables.
**B** Lack of input validation on user input.
**C** A virus attached to an email message.
**D** A program that captures keystrokes.

**17** A software system that has the ability to recover in a timely manner following an unexpected event has displayed which **one** of the facets of the Trustworthy Software Foundation (TSFdn)?

**A** Resilience.
**B** Reliability.
**C** Availability.
**D** Safety.

**18** When a piece of software is the TOE in a security case, which of the following would **NOT** appear as evidence?

**A** The source code for the software including all programmers' comments.
**B** The results of rigorous buffer overflow testing carried out on the software.
**C** A justification of the robustness of the tests used to check for buffer overflows.
**D** A description of the best practice training that the programmers have received.

**19** Which of the following would be a typical top-level claim in a security case?

**A** System X is secured by a firewall.
**B** System X is acceptably secure.
**C** System X is secure.
**D** System X passed all testing.

**20** An administrator has implemented password ageing and complexity on an IT system. Which of the features of core IT security design principles and facets of the Trustworthy Software Foundation (TSFdn) has this deployed?

**A** Fail-safe defaults and safety.
**B** Least privilege and security.
**C** Open design and resilience.
**D** Fail-safe defaults and reliability.

**-End of Paper-**