



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 sample 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 Security by Design Principles can mitigate this?
- A Defence in depth.
 - B Open design.
 - C Fail-safe defaults.
 - D Economy of mechanism.
- 2 Which of the following design aspects will reduce the security risk of application exception errors?
- A Fail securely.
 - B Keep security simple.
 - C Separation of duties.
 - D Defence in depth.
- 3 Which of the following IT security design principles is **MOST** closely related to controlling access to data?
- A Defence in depth.
 - B Separation of duties.
 - C Establish secure defaults.
 - D Least privilege.
- 4 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.
- 5 Under the Trustworthy Software Framework, which two factors are used to determine the required trustworthy level (TL)?
- A Software audience and baseline.
 - B Control set and threat model.
 - C Threat model and baseline.
 - D Software purpose and control set.

- 6 Under the Trustworthy Software Framework (TSF), which software audience type requires the use of Trustworthy Level (TL) 1 or 2?
- A Mass market with Implicit Need (M/I).
 - B Mass market with Explicit Need (E/I).
 - C Niche with Explicit Need (N/E).
 - D No requirement for Trustworthy Software.
- 7 Which of the following is **NOT** a feature of security architecture?
- A Considers the system's ability to meet business objectives.
 - B Addresses the potential risks involved in a particular environment.
 - C Specifies when and where to apply access controls in a system.
 - D Considers the interaction between components in an IT system.
- 8 Using a zoned or segmented network architecture is an initiative under which NCSC secure design principle?
- A Establish the context.
 - B Make disruption difficult.
 - C Reduce the impact of compromise.
 - D Introduce barriers to entry.
- 9 COBIT 5 processes are split into 5 domains. Which 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.
- 10 What is the **PRIMARY** characteristic of the SABSA model?
- A The vendor-neutral nature of the SABSA model implies that layers of abstraction may be removed.
 - B Each item in the SABSA matrix comes from the analysis of business requirements for security.
 - C The SABSA model is not generic and is only suitable for organisations operating a single-vendor policy.
 - D The rows in the SABSA model contain responses related to following classifications; contextual, conceptual, logical, physical and detailed.

- 11 An organisation has recently purchased a new commercial Intrusion Prevention System (IPS). What is the **BEST** source of guidance to inform initial implementation?
- A NCSC.
 - B DHS.
 - C The product vendor.
 - D Google.
- 12 Which organisation authors and maintains the comprehensive Cybersecurity Framework, consisting of the Identify, Protect, Detect, Respond, and Recover components?
- A NCSC.
 - B NIST.
 - C DHS.
 - D COBIT.
- 13 A system owner declares that "the system is adequately secure against all medium rated threats". What is the **BEST** instrument to use to validate this claim?
- A A security case.
 - B A Common Criteria profile.
 - C A FIPS profile.
 - D A security assessment.
- 14 In the context of a security case, firewalls, anti-virus, web proxy and role-based access control systems are all of types of what?
- A Security objectives.
 - B Organisational controls.
 - C Implementation activities.
 - D Technical controls.
- 15 Within a security case, staff awareness and information security training would be considered which type of control?
- A Organisational.
 - B Technical.
 - C Policy.
 - D People.

- 16 What is the relationship between Common Criteria and security cases?
- A Security case results may be used in a Common Criteria as evidence of assurance.
 - B There is no difference between Common Criteria and security cases.
 - C Common Criteria results may be placed in security cases as evidence of assurance.
 - D An enterprise may choose between Common Criteria or a security case as necessary.
- 17 A security case has a requirement to ensure that design elements related to cryptography meet USA government baseline standards. Which resource will provide the **BEST** reference for the security case?
- A FIPS-140-2.
 - B EAL-1.
 - C EAL-2.
 - D FIPS-120-1.
- 18 An attacker appearing to be a legitimate user to access system resources is an example of which STRIDE threat concept?
- A Masquerading.
 - B Spoofing.
 - C Scamming.
 - D Subverting.
- 19 An attacker sniffing clear-text network traffic to eavesdrop is which type of STRIDE threat?
- A Tampering.
 - B Information disclosure.
 - C Capturing.
 - D Elevation of privilege.

- 20** An organisation has just acquired another business and is planning to integrate its IT systems into those of the parent company. What is the **BEST** course of action to take ahead of integrating the two systems?
- A** Review the security accreditation of the new system.
 - B** Expand and re-review the company threat model, including the new system.
 - C** Just connect the two systems.
 - D** Abandon both systems and design a new one.

-End of Paper-