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

Sample Paper

Record your surname/ last/ family name and initials on the Answer Sheet.

Sample paper only. 40 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 26/40.

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.

21 An organisation is implementing a new network security solution and decides to install firewall devices manufactured by two different vendors. Which security design principle is being followed?

A Separation of duties.
B Defence in depth.
C Fail securely.
D Least privilege.

22 A technical security control that continues to provide security capability following a hardware failure is an example of which design principle?

A Fail safe.
B Defence in depth.
C Fail securely.
D Secure defaults.

23 A software system that has the ability to recover in a timely manner following an unexpected event has displayed which of the facets of the Trustworthy Software Framework?

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

24 Which of the following TSF features is **MOST** related to fail-safe defaults?

A Reliability.
B Resilience.
C Security.
D Availability

25 Under the TSF Framework, what is the control set requirement for Trustworthy Level 2 (TL2)?

A No requirement.
B TS Baseline (TSB).
C TS Enhanced (TSEE).
D TS Assessed (TSA).

26 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.

27 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.

28 Reducing the attack surface of a system is a recommendation under which NCSC secure design principle?

A Reduce the impact of compromise.
B Make disruption difficult.
C Establish the context.
D Making compromise difficult.

29 Framework, Process Descriptions, Control Objectives, Management Guidelines and Maturity Models are the core components of which security framework?

A COBIT.
B NIST.
C SABSA.
D TOGAF.

30 Which enterprise security framework provides a coherent set of rules and templates, known as 'viewpoints' or ‘views’, including Strategic, Operational, Service Oriented and Technical views?

A TOGAF.
B MODAF.
C NIST.
D COBIT.

31 Which organisation is responsible for overseeing the Certified Assisted Products (CAPS) cryptographic guidance program?

A NIST.
B ISO.
C NCSC.
D COBIT.

32 The use of a well-defined security case is **MOST LIKELY** to prevent which of the following from occurring?

A Security being bolted-on after implementation.
B Security being considered in the design phase.
C Security being removed after implementation.
D Security being included across the system lifecycle.

33 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.

34 During the development of a security case, the security team realise that the company's IT usage policy needs extensive amendments. Which of the following would be a consequence of implementing the new policy?

A A reduced level of attacks against the system.
B Staff training to cover the new measures.
C More security staff must be employed.
D Greater security of company data and assets.

35 Which section of a security case is used to document the drivers, stakeholders and wider organisational requirements that lead to the requirement for the security case itself?

A Business context.
B Stakeholder management.
C Legal and regulatory environment.
D Cost benefit considerations.

36 A UK CNI organisation is building a security case for a system that relies heavily on cryptographic elements. Which external resource is **BEST** suited to assist with evaluating the security case?

A Common Criteria.
B CIS Benchmarks.
C SANS Critical Controls.
D NCSC CAPS.

37 Degrading the availability of a service by flooding it with network traffic is an example of which STRIDE threat concept?

A Denial of access.
B Tampering.
C Denial of availability.
D Denial of service.

38 The STRIDE concept of information disclosure can be used to threat model violations of which security property?

A Confidentiality.
B Integrity.
C Availability.
D Exposability.

39 An anti-virus company has recently updated their virus signatures to block the latest banking trojan. What is the **MOST LIKELY** response from the threat actors?

A Cease development of the trojan.
B Contact the anti-virus vendor to complain.
C Update the trojan to evade the anti-virus system.
D Develop an entirely new trojan.

40 A commercial web proxy appliance used by your organisation has become end-of-life and is no longer supported by the vendor. What is the **MOST LIKELY** impact on the threat model for this security control?

A The existing threat model will remain the same regardless of vendor support.
B A brand new threat model should be created to address the change.
C The threat model will need updating to assess the impact of a new vulnerability being released.
D The threat model should be deprecated as it requires vendor support.

-End of Paper-