

# City & Guilds Level 4 End-point Assessment for Cyber Security Technologist (9661-12 / 9661-13 / 9661-14)

Standard: ST1021

EPA Plan: Version AP02 and Version 1.1

Sample Test B  
February 2026 Version 1.2

## Sample Knowledge Test

Sample paper, multiple choice answer sheet and mark  
scheme

Version and date	Change detail	Section
V 1.0 June 2022	Initial input of data	Document
V 1.1 April 2025	Update of titling convention	Title page and footer
V1.2 February 2026	Update of version number, adding V1.1	Title page

## Contents

---

<b>1</b>	<b>Introduction</b>	<b>4</b>
	What is in this document	4
	How to use the forms	4
<b>9661-401</b>	<b>End-point Assessment – Knowledge test (Sample Test B)</b>	<b>5</b>
<b>9661-401</b>	<b>End-point Assessment – Knowledge test (Sample Test B) answer sheet</b>	<b>12</b>
<b>9661-401</b>	<b>End-point Assessment Knowledge Test (Sample Test B) – Multiple Choice Mark Scheme</b>	<b>13</b>

---

# 1 Introduction

## What is in this document

This document contains the Sample Knowledge test for the City & Guilds Level 4 Cyber Security Technologist Multiple Choice EPA- Knowledge test (Sample Test B).

## How to use the forms

The following documents are included:

- Sample questions
- Multiple choice answer sheet
- Mark scheme

Apprentices should be provided with the sample questions and the answer sheets.

The mark scheme is to be used by employers/ providers/tutors to mark the completed tests.

## 9661-401 End-point Assessment – Knowledge test (Sample Test B)



**Test duration: 60 minutes**

**You should have the following for this test:**

- a pen with black or blue ink
- multiple-choice answer sheet.

**Read the following notes before you answer any questions:**

- Attempt all questions
- If you find a question difficult, leave it and return to it later.

**This paper contains 40 multiple choice questions worth 1 mark each.**

**This question paper is the property of City & Guilds.**

### **How to complete the multiple choice answer sheet**

Each multiple choice question shows four possible answers (lettered 'a', 'b', 'c' and 'd'); only **one** is correct.

Decide which one is correct and mark your answer on the answer sheet with your pen.

For example, if you decide 'b' is correct, mark your answer with a cross like this:

1 a  b  c  d

If you change your answer, cancel your first choice by filling in the box; then put a cross in the answer which you have now decided is correct, like this:

1 a  b  c  d

## 9661-401 End-point Assessment - Knowledge Test (Sample Test B)

1. Which layer of the OSI model is responsible for maintaining a reliable connection?
  - a) Physical layer.
  - b) Data link layer.
  - c) Network layer.
  - d) Transport layer.
  
2. At which layer of the OSI Model does Bluetooth transfer data between devices?
  - a) Physical layer.
  - b) Network layer.
  - c) Data link layer.
  - d) Transport layer.
  
3. Which of the following is a widely adopted protocol designed to facilitate privacy and data security for communications over the Internet?
  - a) DNS.
  - b) SNMP.
  - c) TLS.
  - d) HTTP.
  
4. Which of the following systems use signature-based **and** statistical anomaly-based detection when monitoring network security?
  - a) Router.
  - b) IDS.
  - c) Switch.
  - d) UPS.
  
5. Which layer of the TCP/IP model is responsible for correcting errors that have occurred at the Physical layer?
  - a) Session.
  - b) Application.
  - c) Transport.
  - d) Data link.
  
6. Why is a TCP SYN flag used?
  - a) It informs the receiving host that the data should be pushed up.
  - b) It finishes the session.
  - c) It initiates the session.
  - d) It indicates the amount of data that is sent on the network.

7. Which of the following IPv4 addresses is class A private address?
- a) 127.0.0.0
  - b) 10.255.255.255
  - c) 172.31.255.255
  - d) 192.168.0.0
8. Which one of the following is the **most** important for network performance management?
- a) VLAN.
  - b) VoIP.
  - c) QoS.
  - d) QOE.
9. In network performance management, what does the term 'error rate' mean?
- a) Variation in packet delay at the receiver of the information over the network.
  - b) Number of corrupted bits expressed as a percentage of the total sent.
  - c) The actual rate at which information is transferred on the network.
  - d) The delay between the sender and the receiver decoding the packets.
10. Which of the following UDP ports is used by SSH?
- a) 5
  - b) 22
  - c) 80
  - d) 110
11. Which of the following port numbers is the default port for SNMP?
- a) 45
  - b) 80
  - c) 161
  - d) 255
12. What port is used by Microsoft Terminal Server?
- a) 53
  - b) 1521
  - c) 3306
  - d) 3389
13. Which of these ports should you forward on a firewall to allow FTP access?
- a) 21
  - b) 80
  - c) 443
  - d) 53

14. Why was TLS developed?
- a) To decrease the complexity of the QoS.
  - b) To address vulnerabilities found in SSLv2.
  - c) To deploy enhanced X.509 certificates.
  - d) To reduce latency when encrypting data.
15. Which of the following protocols is commonly used to provide a secure connection to a Router's command line interface (CLI)?
- a) ARP.
  - b) SSH.
  - c) SNMP.
  - d) LDAP.
16. Which one of the following is a **true** statement about remote access VPN?
- a) Easy to scale for growing environments.
  - b) Increases the connection speed.
  - c) Ideal for networks with large numbers of users.
  - d) Works best for a small number of users.
17. Which of the following is an **advantage** offered by VLANs?
- a) Combining multiple collision domains into a single entity reduces broadcast traffic.
  - b) Allows a flexible network design grouping users by department rather than by physical location.
  - c) The use of MAC addresses increases the transmission speed on local networks.
  - d) When using FTP to establish a trunk, latency between networks is decreased as traffic is filtered.
18. Which of the following VLANs can be deleted when configuring a switch?
- a) VLAN 1.
  - b) VLAN 2 – 1001.
  - c) VLAN 1002 – 1005.
  - d) VLAN – 1006 – 4094.
19. A network engineer has been tasked with setting up a number of Bluetooth PANs within an organisation to allow the implementation of a BYOD policy. Which of the following is a major **disadvantage** associated with setting up multiple PANs in an organisation?
- a) Administrators can check user's personal data files when they are logged on remotely.
  - b) It requires more time to resolve issues due to the use of multiple wireless technologies.
  - c) The PANs may cause interference on other networks using the same frequency range.
  - d) Maintaining the PANs is a difficult task that requires skilled network administrators.

20. Tree topology is a combination of which topologies?
- Bus and Star.
  - Hybrid and Mesh.
  - Bus and Ring.
  - Hybrid and Star.
21. There are limits to the protection provided by Cryptography. Which of the following issues usually **cannot** be addressed by implementing cryptography?
- Spoofing.
  - Poor system design.
  - Regulatory penalties.
  - Forgeries.
22. A company plans to implement email encryption. What method of encryption is **most** commonly used in this scenario?
- Elliptic Curve Cryptography.
  - Public Key Infrastructure.
  - Symmetric Encryption.
  - Quantum Computation.
23. A password is hashed in a database. How could a database administrator retrieve this password?
- Follow all steps in the reset password procedure.
  - Recreate the username table in the database.
  - There is no known method to reverse this process.
  - Put the hashed password into a website.
24. Which of the following is **true** of the Transposition Cipher Technique?
- Plain text characters are rearranged with respect to the position.
  - Plain text characters are replaced with numbers and symbols.
  - A Character's identity is changed while its position is unchanged.
  - Caesar Cipher is a common example of Transposition Cipher.
25. Which cryptography system was pioneered in the late 1970's by two programmers and a mathematician?
- One-way functions.
  - Symmetric ciphers.
  - Pseudo-random functions.
  - Asymmetric keys.
26. Which of the following mechanisms was designed to prevent a hacker from impersonating a website by using fraudulent Certificates?
- Public key pinning.
  - Private key pinning.
  - PGP.
  - GPG.

27. If a PKI private key is compromised, what action should the Certificate Authorities take?
- a) Publish and validate a brand new certificate.
  - b) Distribute a domain validated certificate.
  - c) Issue a root certificate revoking the previous one.
  - d) Revoke the certificate and add it to a deny list.
28. Which of the following is a characteristic of a private key?
- a) The private key mechanism is slower than the public key.
  - b) Algorithms rely on one key to both encrypt and decrypt.
  - c) The private key is never shared between two parties.
  - d) The private key is used for part of the encryption process.
29. What name is given to the system that performs a real-time lookup of a digital certificate's status?
- a) Certificate Revocation List (CRL).
  - b) Online Certificate Status Protocol (OCSP).
  - c) Real-Time CA Verification (RTCAV).
  - d) CA Registry Database (CARD).
30. Which of the following provides recommended baseline security requirements for the use and operation of PKI components, including Certificate Authority and Registration Authority?
- a) Access Point.
  - b) Distribution Point.
  - c) Certificate Policy.
  - d) Laissez Passer.
31. What type of encryption can verify the authenticity of an email sender and enforce non-repudiation?
- a) Elliptic encryption.
  - b) Asymmetric encryption.
  - c) Symmetric encryption.
  - d) Private encryption.
32. What is the term for a trusted third-party storage solution that provides a backup source for cryptographic keys?
- a) Key Escrow.
  - b) Recovery Agent.
  - c) CA.
  - d) TPM.
33. Which digital certificate format is commonly used to store private keys?
- a) .P12
  - b) .P7B
  - c) .PFX
  - d) .CER

34. Where would a hardware security module (HSM) be used?
- a) Removable / external hardware based.
  - b) When implementing full disc encryption.
  - c) High-end mission-critical servers.
  - d) Exchanging payment information with biometric authentication.
35. Which law has been broken by someone who has hacked into an email system?
- a) The Copyright, Designs and Patents Act.
  - b) Computer Misuse Act.
  - c) Electronic Communications Act.
  - d) The Data Protection Act.
36. An organisation develops a very profitable product. What is the **most** effective way to protect their product design?
- a) Invest in resources needed to gain market share as quickly as possible.
  - b) Offer their competitors an incentive not to release a similar product.
  - c) Bring a legal challenge if a competitor releases a similar product.
  - d) Contact the Intellectual Property Office to register a patent.
37. Which of the following laws enables an individual to find out details of an MP's expenses?
- a) Freedom of information Act.
  - b) Electronic Communications Act.
  - c) Official Secrets Act.
  - d) Regulation of Investigatory Powers Act.
38. When referring to the ITAR commerce control list, what are dual-use items?
- a) Dual-use exports involve technology that has both air and sea applications.
  - b) Dual-use exports involve technology that has both commercial and military use.
  - c) Dual-use exports involve technology that has more than one source of origin.
  - d) Dual-use exports involve technology that has more than one application.
39. When an organisation is subject to the terms of RIPA, what is a common concern for the organisation's employees?
- a) Reduction in salary.
  - b) Resourcing for events.
  - c) Working hours regulations.
  - d) Invasion of Privacy.
40. When did the Computer Ethics Institute publish a code of ethics for computer users?
- a) 1988.
  - b) 1990.
  - c) 1992.
  - d) 2000.

# 9661-401 End-point Assessment – Knowledge test (Sample Test B) answer sheet

Candidate name:

*First name*

*Last name*

*(Please print)*

Date of test:

*dd / mm / yy*

1 a  b  c  d

21 a  b  c  d

2 a  b  c  d

22 a  b  c  d

3 a  b  c  d

23 a  b  c  d

4 a  b  c  d

24 a  b  c  d

5 a  b  c  d

25 a  b  c  d

6 a  b  c  d

26 a  b  c  d

7 a  b  c  d

27 a  b  c  d

8 a  b  c  d

28 a  b  c  d

9 a  b  c  d

29 a  b  c  d

10 a  b  c  d

30 a  b  c  d

11 a  b  c  d

31 a  b  c  d

12 a  b  c  d

32 a  b  c  d

13 a  b  c  d

33 a  b  c  d

14 a  b  c  d

34 a  b  c  d

15 a  b  c  d

35 a  b  c  d

16 a  b  c  d

36 a  b  c  d

17 a  b  c  d

37 a  b  c  d

18 a  b  c  d

38 a  b  c  d

19 a  b  c  d

39 a  b  c  d

20 a  b  c  d

40 a  b  c  d

Number of correct answers:  / 40

## 9661-401 End-point Assessment Knowledge Test (Sample Test B) – Multiple Choice Mark Scheme

Grading:

**Pass** 25 marks (62.5%)

<b>Question no</b>	<b>Key</b>	<b>Question no</b>	<b>Key</b>
1	<b>D</b>	21	<b>B</b>
2	<b>A</b>	22	<b>B</b>
3	<b>C</b>	23	<b>C</b>
4	<b>B</b>	24	<b>A</b>
5	<b>D</b>	25	<b>D</b>
6	<b>C</b>	26	<b>A</b>
7	<b>B</b>	27	<b>D</b>
8	<b>C</b>	28	<b>C</b>
9	<b>B</b>	29	<b>B</b>
10	<b>B</b>	30	<b>C</b>
11	<b>C</b>	31	<b>B</b>
12	<b>D</b>	32	<b>A</b>
13	<b>A</b>	33	<b>C</b>
14	<b>B</b>	34	<b>C</b>
15	<b>B</b>	35	<b>B</b>
16	<b>D</b>	36	<b>D</b>
17	<b>B</b>	37	<b>A</b>
18	<b>B</b>	38	<b>B</b>
19	<b>C</b>	39	<b>D</b>
20	<b>A</b>	40	<b>C</b>