



UNIVERSITI TEKNOLOGI MARA
MARKING SCHEME

COURSE	:	COMPUTER SECURITY
COURSE CODE	:	CSC662
EXAMINATION	:	OCTOBER 2026 (MOCK)
TIME	:	3 HOURS

MARKING SCHEME NOTES

1. This marking scheme accompanies the CSC662 mock paper (October 2026).
Computed answers show working; theory answers are supported by lecture slides (not lecturer-marked); verbatim quotes are omitted in this public build; slide citations are retained.
2. Supported theory marking points quote the lecture decks; any unresolved slot would remain a visible placeholder.
3. Part A = $10 \times (2 + 6)$; Part B = $2 \times (5 + 5)$; total = 100 marks.
4. Computed: 3 slot(s). Supported theory: 19 slots. Placeholders: 2.
Questions and answers are for local study use only.
5. Near-copy rejection used all 35 past papers; style widening is recorded per slot.

FOR MARKERS' USE ONLY

This marking scheme consists of N printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

Labels: computed / supported by lecture slides (not lecturer-marked) / placeholder. No official marking scheme exists for the real CSC662 papers; this is generated for the mock.

Entailment labels: supported = the private quote directly supports the point (or the point passed the stem-overlap gate); partly supported = partial/ambiguous support; not supported = no support. Quote text is omitted here; verdicts come from private verification.

Part A: $10 \times (2 + 6) = 80$ marks. Part B: $2 \times (5 + 5) = 20$ marks. Total: 100 marks. Slots: 3 computed, 19 supported by lecture slides, 2 placeholder.

Methods: computed answers use verified solvers. Theory answers are supported by lecture slides (not lecturer-marked). Each point carries a deck/slide citation and overlap score; verbatim quote text is omitted from this public build. Low overlap is flagged for human review.

PART A - QUESTION 1

A1a - 2 marks - computed - matches lecture slides 5-9 (Caesar shift 3 examples)

Question:

Using Caesar Cipher technique, decrypt the following ciphertext with a shift of 7 (replace each letter with the one 7 positions to the left).

KLCPJLYLABYULKHUKDPWLKVUL

Answer: DEVICERETURNEDANDWIPIEDONE

Working:

```

K (10) -7 mod 26 -> D
L (11) -7 mod 26 -> E
C ( 2) -7 mod 26 -> V
P (15) -7 mod 26 -> I
J ( 9) -7 mod 26 -> C
L (11) -7 mod 26 -> E
Y (24) -7 mod 26 -> R
L (11) -7 mod 26 -> E
A ( 0) -7 mod 26 -> T
B ( 1) -7 mod 26 -> U
Y (24) -7 mod 26 -> R
U (20) -7 mod 26 -> N
L (11) -7 mod 26 -> E
K (10) -7 mod 26 -> D
H ( 7) -7 mod 26 -> A
U (20) -7 mod 26 -> N
K (10) -7 mod 26 -> D
D ( 3) -7 mod 26 -> W
P (15) -7 mod 26 -> I
W (22) -7 mod 26 -> P
L (11) -7 mod 26 -> E
K (10) -7 mod 26 -> D
V (21) -7 mod 26 -> O
U (20) -7 mod 26 -> N
L (11) -7 mod 26 -> E

```

Suggested marks: 1 mark for identifying the cipher/shift direction; 1 mark for the complete plaintext.

Confidence: computed - matches lecture slides 5-9 (Caesar shift 3 examples).

A1b - 6 marks - PLACEHOLDER

Topic: classical ciphers; command: Describe

Status: placeholder - no supported question passed verification.

Reason: A1b point 6: marking point is a verbatim copy of its quote; phrase the point as an answer requirement, not as copied slide text

PART A - QUESTION 2

A2a - 2 marks - supported by lecture slides (not lecturer-marked)**Question:**

List two transposition cipher techniques covered in the lecture and, for each, state how the cipher-text is produced from the plain-text.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Columnar transposition: the plain-text is placed into the rows of a matrix and the cipher-text is then read out column by column.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 20 031 - Classical Cryptography::s20::1	supported (stem gate)	0.77
2	Rail fence: the plain-text is written in a zigzag pattern across rows, and the cipher-text is obtained by reading the letters off row by row.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 25 031 - Classical Cryptography::s25::1	supported (stem gate)	0.71

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 031 - Classical Cryptography, slide 20; 031 - Classical Cryptography, slide 25

A2b - 6 marks - computed - matches lecture slide 15 (standard tableau)**Question:**

Decrypt the following ciphertext using the Vigenere cipher with the key CIPHER. Use the standard 26 x 26 Vigenere tableau, writing the key over the message and repeating it as necessary.
UMRBVVNWVPREQE

Answer: SECURELOGINNOW

The 26 x 26 Vigenere tableau is printed in the question paper.

Working:

Standard 26 x 26 tableau, A=0; key repeated over the ciphertext.

Ciphertext: UMRBVVNWVPREQE

Key: CIPHERCIPHERCI

Letter-by-letter: $C - K \bmod 26 = P$

U (20) - C (2) = 18 -> S

M (12) - I (8) = 4 -> E

R (17) - P (15) = 2 -> C

B (1) - H (7) = 20 -> U

V (21) - E (4) = 17 -> R

V (21) - R (17) = 4 -> E

N (13) - C (2) = 11 -> L

W (22) - I (8) = 14 -> O

V (21) - P (15) = 6 -> G

P (15) - H (7) = 8 -> I

R (17) - E (4) = 13 -> N

E (4) - R (17) = 13 -> N

Q (16) - C (2) = 14 -> O

E (4) - I (8) = 22 -> W

Plaintext: SECURELOGINNOW

Suggested marks: 1 mark for the key/table setup; 4 marks for the letter-by-letter working; 1 mark for the complete answer.

Confidence: computed - matches lecture slide 15 (standard tableau).

PART A - QUESTION 3**A3a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

State TWO (2) facts about the chain of trust in the Trusted Computing architecture, including how measurements are recorded and where the chain begins.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the chain measures and validates the following stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.60
2	The measurements produced during the chain are stored in Platform Configuration Registers on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.56

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 073 - Trusted Computing, slide 8

A3b - 6 marks - supported by lecture slides (not lecturer-marked)**Question:**

State SIX (6) facts about the two primary system components of the Next Generation Secure Computing Base (NGSCB), covering the Nexus and the Nexus Computing Agent (NCA).

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	NGSCB has two primary system components, namely the Nexus and the Nexus Computing Agent (NCA).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	partly supported	0.14 LOW
2	The Nexus is a special kernel that forms the core of the trusted operating environment.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.62
3	The Nexus is a security kernel that is authenticated on boot.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.80
4	The Nexus authenticates trusted programs.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.75
5	The Nexus provides the application interface to the TPM and does not trust the OS.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.38 LOW
6	The Nexus Computing Agent is a trusted software component that runs in trusted mode and communicates with the Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.62

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 073 - Trusted Computing, slide 13; 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 4**A4a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

Explain two ways in which the Chinese Wall model differs from traditional access control policies, referring to the type of concern it addresses and how access rights behave over time.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall policy is designed to address a very specific concern, namely conflicts of interest involving a consultant or contractor.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported (stem gate)	0.92
2	Access rights in the Chinese Wall model change dynamically, since what a subject may access depends on the history of its past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.61

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 024 - Formal Security Model, slide 24; 024 - Formal Security Model, slide 27

Status: computed placeholder - no question generated for this type.

PART A - QUESTION 5

A5a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

List the TWO (2) stages that make up the authentication process in a biometric system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage, in which master characteristics are acquired, created and stored.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.50
2	The authentication stage, in which acquisition is repeated, a comparison is made and a decision is reached.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.62

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 072 - Biometrics and Authentication, slide 5

A5b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

A bank plans to deploy biometric authentication at its branch counters. Explain the different categories of biometric technologies and the practical issues that must be considered when choosing a biometric mechanism for this deployment.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that biometric applications are divided into two sectors, namely physiological and behavioural.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.57

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Give examples of physiological biometrics such as iris, fingerprints, hand, retinal and face recognition.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.60
3	Give examples of behavioural biometrics such as voice, typing pattern and signature.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.57
4	Explain that a biometric is a physiological or behavioural characteristic that can distinguish one person from another and can be used for identification or verification.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	1.00
5	Note that fingerprint biometrics suffer from disadvantages such as racial issues, dirt, grime and wounds, and finger placement.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	supported (stem gate)	0.54
6	Note that fingerprint systems can be spoofed, so liveness detection is important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	supported (stem gate)	0.50

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7

PART A - QUESTION 6

A6a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) typical locations where network-based IDS sensors are placed in a network.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor can be positioned just inside the firewall.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.50
2	A sensor can be positioned on the DMZ.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.25 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples n<3; widened via topic+marks (any command).

Citations: 062 - Intrusion Detection System, slide 7

A6b - 6 marks - supported by lecture slides (not lecturer-marked)**Question:**

Explain six (6) preventive network security mechanisms that an organization can deploy to protect its network, describing for each mechanism how it contributes to preventing or limiting security attacks.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall filters traffic entering and leaving the network according to predefined security rules.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported	0.30 LOW
2	A proxy server improves data security and network performance by acting as a firewall and web filter, sharing connections and caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.79
3	Network segmentation creates boundaries between segments whose assets share a common function, risk or role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.75
4	A remote access VPN gives individual hosts or clients secure access to the organization network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	Zero Trust Network Access restricts each user to only the access and permissions needed for their role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.50
6	IDS/IPS detect or prevent attacks such as brute force, denial-of-service and exploitation of network vulnerabilities.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.85

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 061 - Network Security, slide 3; 061 - Network Security, slide 4

PART A - QUESTION 7**A7a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

State TWO (2) characteristics of a Trojan horse as a type of malware.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans typically disguise themselves as useful or benign software.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Trojans steal private information from the infected machine.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.33 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 051 - Software Security, slide 12

A7b - 6 marks - supported by lecture slides (not lecturer-marked)**Question:**

Describe six (6) techniques used by malware to propagate itself or to conceal its presence on an infected system, and explain the impact of each technique on the victim.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A boot sector virus saves the original master boot record in a safe location before overwriting it with an infected version.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 8 051 - Software Security::s08::1	partly supported	0.31 LOW
2	A COM executable virus appends its virus body to a program and replaces the program entry point with a jump to the virus body.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.70
3	An EXE executable virus overwrites a program header so that the entry point switches to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.67
4	A rootkit masks malicious processes and software in the infected system to ensure privileged remote access.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	1.00
5	A rootkit is usually installed after a vulnerability has been found and detected, so the infected computer stays under the malware author's control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.87
6	Spyware steals user logins and passwords, documents sites visited, logs keystrokes and redirects browsers, leading to identity theft and compromised bank information.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.61

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 8; 051 - Software Security, slide 9

PART A - QUESTION 8

A8a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how a buffer overflow arises in a program such as the web server function that copies input into a fixed-size local buffer, and state what an attacker can achieve by exploiting it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The overflow occurs because the copying routine does not verify the length of the input string, so a longer string than the buffer can hold spills over.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.17 LOW
2	By controlling the overflowing content, the attacker can overwrite the saved return address with an arbitrary value and thereby hijack the execution flow of the program.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.69

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 051 - Software Security, slide 21; 051 - Software Security, slide 23

A8b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Windows is often described as offering rich built-in security, yet it remains a frequent target of attack. Explain six aspects of Windows security mechanisms, covering the overall nature of these mechanisms, the directory service for organising resources, how subjects and their credentials are handled, the registry's security role, the historical security milestones, and the risk that complexity itself creates.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides complex built-in mechanisms covering user accounts, object management and access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.75
2	Discretionary access control in Windows allows fine-grained control over diverse entities in the OS and in applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.55
3	Active Directory, introduced with Windows 2000, is an LDAP-like directory service used to organise system resources.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.91
4	In Windows, subjects are processes and threads, and their security credentials are held in a token.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.50
5	The registry is a hierarchical database holding critical system information, including security-related hives such as SAM and security logs.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 4 041 - Windows Security::s04::1	partly supported	0.36 LOW
6	The complexity of Windows security is double-edged, since misconfiguration and implementation bugs can cause severe security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.54

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 041 - Windows Security, slide 11; 041 - Windows Security, slide 21; 041 - Windows Security, slide 4; 041 - Windows Security, slide 6

PART A - QUESTION 9

A9a - 2 marks - PLACEHOLDER

Topic: attacks/malware; command: Explain

Status: placeholder - no supported question passed verification.

Reason: A9a: sub-angle not followed; use one of ['confidentiality', 'integrity', 'availability', 'impact', 'harm', 'damage']

A9b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Discuss the Samy worm as a case study of a self-propagating web malware attack. In your answer, explain how the worm injected and spread its payload, how victims were drawn into triggering the malicious script, and what the outcome of the outbreak was.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by manipulating the page body through <code>document.body.innerHTML</code> .	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.58
2	The worm obtained the victim's list of friends by issuing a GET request on a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.22 LOW
3	The worm added Samy as a friend by performing an XML-HTTP request against the <code>addFriends</code> page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.64
4	Any user visiting an infected profile had their own profile and friends list infected, so the worm spread from visitor to visitor.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.46 LOW
5	The outbreak ultimately infected approximately one million MySpace profiles, showing the scale a web worm can reach.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.15 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Users were lured into executing the malicious script inadvertently, for example by clicking an emailed link or an infected image.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	partly supported	0.31 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples n<3; widened via topic+marks (any command).

Citations: 052 - Web Security, slide 13; 052 - Web Security, slide 15

PART A - QUESTION 10

A10a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain two password security controls that an administrator can apply to password files and accounts in order to strengthen password-based authentication.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control should be applied to the password files so that they are protected from unauthorised reading.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	partly supported	0.40 LOW
2	Accounts should be de-activated after multiple failed login attempts to resist guessing attacks.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.55

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 022 - Identification and Authentication, slide 12

A10b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Refer to your answer in (a). Based on the scenario in (a), explain how Kerberos, smartcards and single sign-on mechanisms can be used to authenticate users across a large distributed environment, giving six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the burden on users by cutting down the number of passwords they must remember.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.17 LOW
2	Single sign-on also saves users time because they type passwords less often.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.18 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Kerberos is an example of a client-server single sign-on architecture.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.57
4	In Kerberos the user presents a user name and password at the client workstation to begin login.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.57
5	Kerberos derives a secret key for the client by hashing the user's password.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.71
6	Smartcards are listed as an alternative authentication mechanism alongside biometrics and two-factor authentication.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 24 022 - Identification and Authentication::s24::1	supported (stem gate)	0.71

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 19; 022 - Identification and Authentication, slide 24

PART B - QUESTION 1

B1a - 5 marks - supported by lecture slides (not lecturer-marked)

Scenario:

A junior developer at a healthcare software firm discovers that a colleague has been copying patients' records into a personal spreadsheet to speed up testing. When challenged, the colleague argues that no written rule forbids it and that the data is only used internally. The firm's management asks the security team to clarify how morals, ethics and laws apply before deciding on any action.

Question:

Explain how morals, ethics and laws differ as guides for judging the colleague's conduct, and then explain how the ACM code would direct the developer's professional behaviour in this situation.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that morals concern traditions of belief about right and wrong conduct, forming the basis of social behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.67
2	Describe ethics as a set of guiding beliefs, standards or ideals held by an individual, group or community.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.80
3	Describe laws as formal rules of conduct imposed by a sovereign authority such as a government on its citizens.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	1.00

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Note that the ACM code requires the professional to respect privacy.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.29 LOW
5	Note that the professional must access computing and communication resources only when authorised or compelled by the public good.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.69

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 071 - Ethics and Computer Security, slide 11; 071 - Ethics and Computer Security, slide 12; 071 - Ethics and Computer Security, slide 5

B1b - 5 marks - supported by lecture slides (not lecturer-marked)

Question:

State five points about the professional code of ethics and conduct that the security team should present to management in the scenario, covering what such a code is, who defines it, an example of a professional body that issues one, and two limitations of relying on it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A professional code of ethics is a documented set of acceptable behaviours for a professional group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.62
2	The code is defined by the group itself rather than imposed from outside.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.25 LOW
3	The ACM is an example of a professional body that has a code of ethics and professional conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.75
4	A limitation is that the code may not reflect the ethics of every member of the group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported (stem gate)	0.78
5	A further limitation is that the code is often not enforceable because it is a code of conduct, not a legal document.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported (stem gate)	0.60

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 071 - Ethics and Computer Security, slide 6; 071 - Ethics and Computer Security, slide 7; 071 - Ethics and Computer Security, slide 9

PART B - QUESTION 2

B2a - 5 marks - supported by lecture slides (not lecturer-marked)**Scenario:**

A hospital's file server stores patient records and administrative documents. The security team is comparing how access rights could be recorded for each file and each user, and wants a structure that is easy to verify and to manage as staff change roles.

Question:

Explain the access control structures available for implementing access policies, covering the access control matrix, access control lists and capabilities, and state the requirements such structures must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify the access control matrix as one of the basic structures for implementing access policies, alongside capabilities and ACLs.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.50
2	State that an ACL describes access rights from the object's point of view, listing which subjects may access that object and how.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.50
3	Give one advantage of the access control matrix, namely that it is clearly defined and easy to verify.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.38 LOW
4	Name the requirements that any access control structure must meet: expressing policies, verifiability of correctness, and scalability with manageability.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.46 LOW
5	Note that in practice the most common instruments are ACLs, capabilities and various abstractions built on them.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	0.73

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Citations: 023 - Access Control and Authorization, slide 10; 023 - Access Control and Authorization, slide 18; 023 - Access Control and Authorization, slide 7; 023 - Access Control and Authorization, slide 8

B2b - 5 marks - supported by lecture slides (not lecturer-marked)**Question:**

Discuss the goals that authorization aims to achieve and the role of the reference monitor in making authorization decisions, relating your discussion to the hospital file server in the scenario.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Authorization must decide, for a given subject, which objects it may access and in what manner.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported	0.44 LOW
2	Authorization must also decide, for a given object, which subjects may access it and in what manner.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported	0.40 LOW
3	The reference monitor is the component that makes the authorization decisions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	1.00
4	Authorization/access control aims to achieve four goals: granting access, limiting access, preventing access, and revoking access.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.70
5	In the Windows architecture, the Security Reference Monitor performs ACL verification in kernel mode.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	partly supported	0.40 LOW

Confidence: supported by lecture slides (not lecturer-marked) - source citation retained; verbatim quote omitted in the public build.

Style confidence: LOW - exact examples $n < 3$; widened via topic+marks (any command).

Citations: 023 - Access Control and Authorization, slide 4; 041 - Windows Security, slide 3

End of marking scheme.