



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: 21 slots. Placeholders: 0.
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 15 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, 21 supported by lecture slides, 0 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 - supported by lecture slides (not lecturer-marked)

Question:

Explain substitution ciphers as a classical cipher family. In your answer, describe how substitution works, what serves as the key, its relation to Shannon's principle of confusion, and its relevance to modern ciphers.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that substitution replaces plaintext letters with other letters.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.80
2	Note that the text produced by the substitution is the ciphertext.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.20 LOW
3	Identify the substitution rule as the key of the cipher.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.67
4	Relate substitution to Shannon's principle of confusion.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.60
5	Explain that the substitution idea is used in modern ciphers.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported (stem gate)	0.75
6	Contrast with transposition, where plaintext is placed into rows of a matrix and ciphertext is read out of columns.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 20 031 - Classical Cryptography::s20::1	supported (stem gate)	0.50

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 4

PART A - QUESTION 2

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

Question:

Explain how a rail fence transposition cipher works, covering both the encryption and decryption processes.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Encryption writes the plaintext in a zigzag pattern across rows and reads letters row by row to form the ciphertext.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 25 031 - Classical Cryptography::s25::1	supported (stem gate)	0.55
2	Decryption rebuilds the empty rail fence table using the known key, fills rows with ciphertext, then reads in zigzag to recover plaintext.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 26 031 - Classical Cryptography::s26::1	partly supported	0.40 LOW

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

Citations: 031 - Classical Cryptography, slide 25; 031 - Classical Cryptography, slide 26

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:**

Explain the two stages of the biometric authentication process and state what happens during each stage.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage involves acquiring the biometric sample, creating the master characteristics and storing them.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported	0.30 LOW
2	The authentication stage involves acquiring a sample, comparing it and making a decision.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported	0.43 LOW

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

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

Describe six points about biometric mechanisms and technologies, covering what a biometric is, how biometric applications are categorised, and the characteristics and drawbacks of specific biometric technologies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A biometric is defined as a physiological or behavioural characteristic of a human being that can distinguish one person from another and can theoretically be used for identification or verification of identity.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.92
2	Biometric applications available today are divided into two sectors.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.86
3	The physiological sector of biometrics includes 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
4	The behavioural sector of biometrics includes 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
5	Iris scanning reads the unique pattern of the iris, which is coloured and visible from far, and it requires no touch, thereby overcoming retinal scanner issues.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.27 LOW
6	Fingerprint biometrics suffer disadvantages such as racial issues, dirt, grime and wounds, finger placement problems, an overly large database to process, and spoofing, making liveness important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	partly supported	0.10 LOW

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

Citations: 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7

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

List two formal security models named in the lecture and, for each, state the specific security concern it is designed to address.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall model (Brewer and Nash) is designed to address conflicts of interest for 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)	0.91

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	The Biba model adds integrity verification on top of access control.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.50

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: 024 - Formal Security Model, slide 27; 024 - Formal Security Model, slide 5

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

PART A - QUESTION 5

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

Question:

State TWO (2) facts about how a chain of trust is established using the Trusted Platform Module (TPM) in a trusted computing platform.

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 this process are stored in Platform Configuration Registers (PCRs) on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.60

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

Citations: 073 - Trusted Computing, slide 8

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

Question:

Explain the roles of the Nexus and the Nexus Computing Agent (NCA) as the two primary system components of the Next Generation Secure Computing Base (NGSCB), and state how the Nexus relates to the TPM and to the operating system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	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
2	The Nexus isolates the normal mode process from the trusted mode process by handling them differently in memory.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.67
3	The Nexus acts as the application interface to the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.60
4	The Nexus is a security kernel that is authenticated on boot and does not trust the operating system.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.40 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	The NCA 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)	0.71
6	The NCA specifications are open-source, allowing developers to create their own agents to run on the trusted platform.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::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: 073 - Trusted Computing, slide 13; 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 6

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

Question:

List two types of malware and, for each, state one characteristic behaviour that distinguishes it, as described in the software security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans masquerade as helpful or harmless programs while stealing private data, deleting files, logging keystrokes or opening the way for further malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.82
2	Worms exploit a vulnerability in the computer system to cause harm, such as corrupting or deleting critical files and consuming excess bandwidth.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	partly supported	0.47 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: 051 - Software Security, slide 12

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

Question:

Discuss six techniques by which malware attacks and propagates through a system, drawing on the software security lecture's account of malware behaviour and infection mechanisms.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Rootkits conceal malicious processes so that the attacker retains privileged remote access after a vulnerability has been exploited.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported	0.46 LOW
2	Spyware performs surveillance of the user, capturing credentials and recording activity such as keystrokes and visited sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported	0.42 LOW
3	A virus can propagate by appending its body to a host executable program.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.50
4	A virus can hijack execution by overwriting the program header so that the entry point switches to the virus code.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.55

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Early malware spread through boot sector infection of disks, as illustrated by Elk Cloner and the Brain Virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.31 LOW
6	The Morris worm propagated by exploiting a debugging feature of sendmail to achieve remote execution across the network.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported	0.36 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: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 7

PART A - QUESTION 7

A7a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain how the classes of threats described in the introduction to computer security affect confidentiality, integrity and availability.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is a threat class involving unauthorized access to information, and it is countered by confidentiality services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.40 LOW
2	Deception and disruption are threat classes that involve modification, and they are countered by integrity services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.10 LOW

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

Citations: 011 - Introduction to Computer Security, slide 10

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

Question:

State six facts about the Samy worm and the cross-site scripting (XSS) attack it exploited, covering how the malicious script was injected, how it spread between users, why the browser permitted it, and the outcome of the incident.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by writing to document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.70
2	It obtained the list of a user's heroes 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	0.43 LOW
3	It added Samy as a friend by performing XML-HTTP on the addFriends page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.88
4	Any visitor to an infected profile had their own profile and friends list infected, and roughly 1,000,000 MySpace profiles were eventually infected.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	partly supported	0.36 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	The root cause is that any web application returning user input without filtering is a potential XSS vulnerability, allowing arbitrary JavaScript to run in the user's browser.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.56
6	In XSS the JavaScript does not originate from the web server but is dynamically injected via a user request and reflected from a third party, which is the cross-site element.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 14 052 - Web Security::s14::1	supported (stem gate)	0.90

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

Citations: 052 - Web Security, slide 13; 052 - Web Security, slide 14; 052 - Web Security, slide 15

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 one using strcpy() and how an attacker can exploit it to hijack execution.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The overflow occurs because strcpy() copies the input without checking its length against the buffer size.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.25 LOW
2	Without bound checking the overspill reaches the adjacent upper stack area, letting the attacker overwrite the return address and hijack the execution flow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	partly supported	0.35 LOW

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:

Describe six Windows security mechanisms and related design considerations that a system administrator must understand when securing a Windows host, covering how subjects are represented, how access to objects is controlled, how resources are organised, and why the complexity of these mechanisms can itself be a risk.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides complex built-in mechanisms for managing user accounts, objects and access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.82
2	Discretionary access control lists allow fine-grained control over diverse entities both in Windows itself and in applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.54
3	The very complexity of Windows security mechanisms can backfire, since misconfiguration and implementation bugs can cause serious security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.50
4	In Windows, the active subjects are processes and threads.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.80

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	A subject's security credentials are held in a token, which maps a principal to a subject and can carry extra security attributes.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	partly supported	0.36 LOW
6	Access rights define what a subject may do to an object and are encoded as a 32-bit mask.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 16 041 - Windows Security::s16::1	partly supported	0.33 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: 041 - Windows Security, slide 11; 041 - Windows Security, slide 16; 041 - Windows Security, slide 21

PART A - QUESTION 9

A9a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) differences between morals and laws as described in the lecture on ethics and computer security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.86
2	Laws are formal rules of conduct imposed by a sovereign authority such as a government on its subjects or 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

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

Citations: 071 - Ethics and Computer Security, slide 5

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

Question:

Refer to your answer in (a). Explain how a professional code of ethics and conduct guides a computing professional, using the ACM code to illustrate six (6) distinct professional obligations.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A code of ethics is a documented set of acceptable behaviours for a professional group, defined by that 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)	0.56
2	The professional body's code identifies which specific actions are appropriate or inappropriate.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.50
3	The ACM, founded in 1947, 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)	0.80

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	The professional should contribute to society and human well-being, recognising all people as stakeholders in computing.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.73
5	The professional should respect privacy and honour confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	partly supported	0.33 LOW
6	The professional should maintain high standards of professional competence, conduct and ethical practice.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.89

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

Citations: 071 - Ethics and Computer Security, slide 11; 071 - Ethics and Computer Security, slide 12; 071 - Ethics and Computer Security, slide 6; 071 - Ethics and Computer Security, slide 7

PART A - QUESTION 10

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

Question:

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

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

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

Question:

Explain six (6) preventive network security mechanisms that an organization can deploy, describing what each mechanism does to protect the network.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall controls incoming and outgoing network traffic according to predetermined security policies.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
2	A proxy server improves data security and network performance by acting as a firewall and web filter, sharing network 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Network segmentation creates boundaries between network segments whose computing 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)	0.77
4	A remote access VPN gives individual hosts or clients remote and secure access to the organization's 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 (ZTNA) restricts each user to only the access and permission required to fulfil the role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.58
6	Intrusion detection/prevention systems detect or prevent network attacks such as brute force attacks, Denial-of-Service attacks and exploits 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 B - QUESTION 1

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

Question:

Explain five password security controls that an organisation can apply to protect user accounts and password files, and state one password policy practice for the root password.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Apply access control 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	0.44 LOW
2	De-activate user accounts automatically after several failed login attempts.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.56
3	Show the time of the user's last login so that unusual access can be noticed.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	partly supported	0.33 LOW
4	Store the password in an encrypted form produced by a one-way hash function.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 8 022 - Identification and Authentication::s08::1	supported (stem gate)	0.88
5	For the root password, adopt a policy that it is only entered locally on the machine it controls.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.56

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: 022 - Identification and Authentication, slide 12; 022 - Identification and Authentication, slide 8

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

Question:

A large organisation wants to reduce the number of passwords its staff must remember and manage. Explain five points about single sign-on and Kerberos that the organisation should consider, covering the motivation for single sign-on, the authentication categories involved, Kerberos design criteria, the initial Kerberos exchange, and the limitations of Kerberos.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the burden on users by cutting down the need to memorise passwords and the time spent typing them.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	partly supported	0.23 LOW
2	Smart cards are classified as a 'something you have' authentication mechanism, alongside security tokens.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 9 022 - Identification and Authentication::s09::1	supported (stem gate)	0.60
3	Kerberos is designed to be transparent, so the user is unaware of any authentication beyond the initial login.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.70
4	In the initial exchange the client sends its user ID and the requested service to the authentication server.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 20 022 - Identification and Authentication::s20::1	supported (stem gate)	0.78
5	Kerberos suffers from being relatively complex to install and from having a single point of failure.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 23 022 - Identification and Authentication::s23::1	partly supported	0.33 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: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 20; 022 - Identification and Authentication, slide 23; 022 - Identification and Authentication, slide 9

PART B - QUESTION 2

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

Scenario:

A security architect is comparing how operating systems and formal models represent access rights. She examines an object-centred list attached to a file, a matrix of subjects against objects, and a capability list held by each subject, and asks how these structures differ in what they make easy to see and easy to revoke.

Question:

State five points about access control structures, covering the three named structures, the requirements

they must satisfy, and the advantages and disadvantages of an access control list.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Name the access control matrix as one of the structures used to implement access policies	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.83
2	Name capabilities, given as C-List, as a second structure	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.25 LOW
3	State that an ACL is an object-centred description of access rights	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.83
4	Give one advantage of ACLs, namely that object access rights are easy to reach	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.57
5	Give one disadvantage of ACLs, namely that revocation is difficult	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported	0.25 LOW

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 7

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

Question:

Referring to the scenario, discuss the authorization goals that an access control system must serve and explain how a reference monitor supports these goals, including the role of the Chinese Wall model in controlling access.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The four authorization goals of access control are granting, limiting, preventing 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)	0.88

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	A reference monitor is the component that makes 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
3	Reference monitors are instruments for realizing access control policies and can be deployed at all levels of the system hierarchy.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	1.00
4	The Chinese Wall model is an access control confidentiality policy that addresses conflicts of interest.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.90
5	Under the Chinese Wall simple security rule, a subject may access an object only if it is within the same company dataset already accessed or belongs to an entirely different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	supported (stem gate)	0.91

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 18; 023 - Access Control and Authorization, slide 4; 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 25

End of marking scheme.