



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: 2 slot(s). Supported theory: 22 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 x (2 + 6) = 80 marks. Part B: 2 x (5 + 5) = 20 marks. Total: 100 marks. Slots: 2 computed, 22 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 - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) differences between morals and laws as forms of conduct guidance for computing professionals.

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.	[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

A1b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Discuss how a professional code of ethics and conduct guides the behaviour of a computing professional, referring to the ACM code and its professional conduct expectations. Support your discussion with six distinct requirements.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify that professional bodies such as the ACM publish a formal code of ethics and professional conduct for computing practitioners.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.55
2	Explain that ethics is a documented set of acceptable behaviours defined by a professional or social 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)	0.67

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	State that the code requires the professional to 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)	0.67
4	Note that the code obliges the professional to 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	0.25 LOW
5	Describe the conduct expectation that the professional maintains high standards of 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
6	Explain that the professional must give thorough evaluations of computer systems and their impacts, including analysis of possible risks.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.82

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 2

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

Question:

Explain how a substitution cipher conceals the original message and what role the substitution rule plays in that process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The cipher works by swapping each plaintext letter for a different letter, producing the ciphertext.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.29 LOW
2	The particular substitution rule applied acts as the secret key of the cipher.	[verbatim slide quote omitted in public build]	031 - Classical Cryptography, slide 4 031 - Classical Cryptography::s04::1	supported	0.29 LOW

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

Citations: 031 - Classical Cryptography, slide 4

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.
 UMRBVVNWWVPREQE

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: UMRBVVNWWVPREQE

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 the two stages of the biometric authentication process and, for each stage, name the activities it involves.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identification stage: involves acquisition, creation of master characteristics, and storage of master characteristics.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.86
2	Authentication stage: involves acquisition(s), comparison, and decision.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.83

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:

State six facts about biometric mechanisms and technologies as covered in the course, covering the definition of a biometric, the two application sectors, the behavioural examples, the physiological examples, the fingerprint process, and the iris scanning advantages.

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Biometric applications available today are categorized 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)	1.00
3	The behavioural category 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)	0.67
4	The physiological category 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)	0.67
5	In fingerprint processing, the print is divided into loops, whorls and arch, and minutiae points (ridge endings) are calculated.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 6 072 - Biometrics and Authentication::s06::1	partly supported	0.46 LOW
6	Iris scanning requires no touch and overcomes retinal scanner issues.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.25 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: 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 6

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 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)	0.89
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) 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 carry out harmful actions such as stealing private data, deleting files, logging keystrokes, or opening the system for further malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.59

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

Citations: 051 - Software Security, slide 12

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

Question:

Explain how malware such as viruses and worms propagate and conceal themselves, giving six distinct techniques or behaviours drawn from the history and mechanics of malware.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Early malware could spread by infecting the boot sector of a disk.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported (stem gate)	0.50
2	A worm can propagate across a network by exploiting a remote execution feature of a service.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	supported	0.22 LOW
3	A COM-file virus appends its body to a program and redirects the program entry point to the virus code.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.50
4	An EXE-file virus overwrites the program header so that execution begins in the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported	0.38 LOW
5	A rootkit hides malicious processes and software so that the infected machine stays under the author's remote control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.50
6	Spyware collects user credentials and activity, for example by logging keystrokes.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported	0.38 LOW

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 7; 051 - Software Security, slide 9

PART A - QUESTION 6

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

Question:

Explain how a network-based intrusion detection system (NIDS) should be architected, with particular reference to where its sensors are placed.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors must be positioned deliberately so that the most valuable assets are defended.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.62
2	Typical sensor locations include just inside the firewall, on the DMZ, on the server farm segment, and on segments linking mainframe or midrange hosts.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	partly supported	0.20 LOW

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

Citations: 062 - Intrusion Detection System, slide 7

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

Refer to your answer in (a). Explain how preventive network security mechanisms such as firewalls, proxy servers, network segmentation and remote access VPNs reduce the workload and exposure of the detection system you described, giving six distinct points.

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, thereby filtering traffic before it reaches the detection system.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.50
2	A proxy server acts as a firewall and web filter, provides shared network connections and caches data to speed up common requests, improving data security and performance.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.83
3	Network segmentation creates boundaries between network segments whose computing assets share a common function, risk or role within the organization.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
4	A remote access VPN provides individual hosts or clients with remote and 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)	0.90
5	Zero Trust Network Access ensures a user only has 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)	0.67
6	The detection system monitors network resources to detect intrusions and attacks that were not stopped by preventive techniques such as firewalls, proxy servers, packet-filtering routers and network segmentations.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 3 062 - Intrusion Detection System::s03::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: 061 - Network Security, slide 3; 061 - Network Security, slide 4; 062 - Intrusion Detection System, slide 3

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

Explain how a chain of trust is established in the Trusted Computing architecture, with reference to the TPM and the measurement of each stage.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the platform measures and validates the following stage, and the resulting measurements are recorded in the TPM's Platform Configuration Registers (PCRs).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.27 LOW
2	The chain begins at the hardware TPM and then proceeds through the software layers (RTM, TPM Software Stack, BIOS, kernel), so that the whole platform ends up verified as being in a trusted state.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.28 LOW

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

Citations: 073 - Trusted Computing, slide 8

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

Describe six (6) components and characteristics of the Next Generation Secure Computing Base (NGSCB), focusing on the Nexus and the Nexus Computing Agent (NCA).

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	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
2	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
3	The Nexus provides 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 does not trust the operating system.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.50
5	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)	0.75
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)	0.82

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

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

PART A - QUESTION 8**A8a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

List two classes of threats and, for each, state the security objective whose violation represents the harm caused to the system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is a threat class in which information is accessed without authorization, harming confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported	0.33 LOW
2	Deception is a threat class involving acceptance of false data, harming integrity.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.44 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: 011 - Introduction to Computer Security, slide 10

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

State six (6) facts about the Samy worm as a case study of a cross-site scripting (XSS) attack, covering how the malicious script was injected, how it spread to other users, and the scale of the infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile using document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
2	The worm 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	0.38 LOW
3	The worm added Samy as a field 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)	0.78
4	Any user visiting an infected user's page had their profile and friends list infected with the JavaScript.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
5	The infection eventually reached about 1,000,000 MySpace profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.71
6	The attacker inserted a malicious string into the website's database through one of the website's forms.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 16 052 - Web Security::s16::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: 052 - Web Security, slide 15; 052 - Web Security, slide 16

PART A - QUESTION 9**A9a - 2 marks - supported by lecture slides (not lecturer-marked)**

Question:

Explain two ways in which an intrusion detection system contributes to detecting and defending against attacks on a computer system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can identify and stop attacks that are currently in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported (stem gate)	0.50
2	An IDS can carry out forensic analysis after an attack has finished.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported	0.30 LOW

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

Citations: 062 - Intrusion Detection System, slide 2

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

Describe six (6) distinct software threat classes or attack techniques that can compromise a computer system, and for each, state the security objective that the attack violates.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Modification of program code is a software threat class that violates integrity.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.25 LOW
2	Viruses and self-replicating code are a software threat class that violates integrity.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.44 LOW
3	Buffer overflow is a software threat class that violates integrity.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 7 011 - Introduction to Computer Security::s07::1	partly supported	0.14 LOW
4	SQL injection is a software threat class that violates confidentiality.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.29 LOW
5	Script injection such as XSS is a software threat class that violates confidentiality.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.33 LOW
6	Format string vulnerabilities are a software threat class that violates integrity.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 2 051 - Software Security::s02::1	partly supported	0.38 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 7; 051 - Software Security, slide 2

PART A - QUESTION 10**A10a - 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 state why this class of

flaw is so widely exploited by attackers.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The overflow occurs because strcpy() copies the input string without checking its length, so a longer string than the destination buffer spills over.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.25 LOW
2	Buffer overflows are among the most widely used exploitation techniques.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::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: 051 - Software Security, slide 23; 051 - Software Security, slide 30

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

Question:

Explain six Windows security mechanisms and features that support user account management, object access control and system protection, and discuss why the complexity of these mechanisms can itself become a security weakness.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows provides elaborate built-in mechanisms for managing user accounts and objects and for enforcing access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.67
2	Discretionary access control in Windows allows detailed, fine-grained control over access to diverse objects both in the OS and in applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.39 LOW
3	The same complexity that gives Windows its power is also a liability, because configuration mistakes and coding bugs can cause serious security breaches.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.31 LOW
4	Windows 2000 introduced Active Directory, Kerberos authentication and a structured security architecture.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 2 041 - Windows Security::s02::1	supported (stem gate)	0.70
5	Windows Vista removed the default administrator mode and added a firewall and Data Execution Prevention.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 2 041 - Windows Security::s02::1	supported	0.18 LOW
6	Active Directory is a directory service that organizes users, groups, credentials, resources, security policies and trust relationships.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	partly supported	0.42 LOW

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

Citations: 041 - Windows Security, slide 2; 041 - Windows Security, slide 21; 041 - Windows Security, slide 6

PART B - QUESTION 1

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

Question:

Discuss the access control structures used to implement access policies, covering the access control matrix, access control lists and capabilities, and the requirements these structures must satisfy.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify the access control matrix, capabilities and access control lists as the named structures for implementing 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)	0.71
2	State the requirements that access control structures must meet, including expressing policies, verifiability, 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	partly supported	0.25 LOW
3	Explain that the access control matrix is a basic structure offering clarity of definition and ease of verification.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	partly supported	0.30 LOW
4	Note the disadvantages of the access control matrix, namely poor scalability and poor handling of changes.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	partly supported	0.22 LOW
5	Describe the access control list as an object-centred description of access rights, giving an example such as a file mapped to a user with read and write rights.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::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: 023 - Access Control and Authorization, slide 10; 023 - Access Control and Authorization, slide 7; 023 - Access Control and Authorization, slide 8

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

Question:

Explain the goals that access control is intended to achieve and the role of the reference monitor in making authorization decisions, including how a reference monitor is realised in the Windows security architecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State the four goals of access control: 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)	1.00

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Explain that the reference monitor is the component that makes authorization decisions for access requests.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.71
3	Describe reference monitors as the instruments for realising access control policies that 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)	0.92
4	Identify the Security Reference Monitor in kernel mode as the Windows component that performs ACL verification.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	partly supported	0.44 LOW
5	Note that in user mode the Local Security Authority handles access tokens (alongside password verification and audit logs).	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.57

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 18; 023 - Access Control and Authorization, slide 4; 041 - Windows Security, slide 3

PART B - QUESTION 2

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

Scenario:

A small company runs a shared Linux server where staff log in with user names and passwords. The administrator is reviewing how password files are protected and how accounts are handled after repeated failed logins, and wants to tighten the password controls in place.

Question:

Explain five password security controls that an administrator can apply to protect user accounts and password files on a multi-user system.

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 an account 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)	0.62
3	Show the time of the user's last login so that unexpected 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Enforce password policies, for example for the root password.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.60
5	Store the password in encrypted form using 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)	1.00

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

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

Question:

The administrator in the scenario wants to reduce the burden of password handling for staff on the shared server. State five points about single sign-on, Kerberos and smart cards as authentication mechanisms that the administrator could rely on.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the need for users to memorise passwords	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.43 LOW
2	Single sign-on reduces the time users spend typing passwords	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.43 LOW
3	Single sign-on can be realised through client-server architectures such as Kerberos and Active Directory	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.50
4	Single sign-on methods such as Kerberos automate authentication in large distributed environments	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 24 022 - Identification and Authentication::s24::1	supported (stem gate)	1.00
5	Smart cards are listed as an alternative user 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)	0.89

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 24

End of marking scheme.