



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: 0 slot(s). Supported theory: 24 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 16 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: 0 computed, 24 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:

Explain the difference between morals, ethics and laws as three distinct forms of guidance for conduct.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning 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)	0.55
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

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

Question:

Explain six ways in which a professional code of ethics and conduct, such as the ACM code, guides the behaviour of a computing professional.

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 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
2	The code is defined by the professional group itself.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.40 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	It 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)	1.00
4	It requires the professional to contribute to society and human well-being, recognising all people as stakeholders.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.70
5	It 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	0.33 LOW
6	It directs the professional to 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

PART A - QUESTION 2

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

Question:

State TWO (2) formal security models that are classified as information flow models, and state the specific concern that the Chinese Wall model is designed to address.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall model is listed as an information flow model concerned with identifying conflicts of interest.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.62
2	The Chinese Wall policy is designed to address the specific concern of conflicts of interest by 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)	1.00

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

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

A2b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Explain the three main access control structures used to implement access policies, namely the access control matrix, access control lists and capabilities, and for each structure state one advantage or disadvantage associated with its use.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The access control matrix is described as a basic control structure for implementing access policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.43 LOW
2	A strength of the access control matrix is that it is clear to define 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	0.25 LOW
3	A weakness of the access control matrix is that it scales poorly and handles changes poorly.	[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	An access control list is an object-centred description of the access rights held on that object.	[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	Access control lists make it easy to see and manage the access rights on an object, including through abstractions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.55
6	Access control lists suffer from a poor overview of a subject's rights and from difficulty in revoking and sharing 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)	0.60

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 8

PART A - QUESTION 3

A3a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

State TWO (2) points about software insecurity and buffer overflows as presented in the Software Security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Software insecurity arises because an attacker can modify system resources that are critical for program execution, such as the instruction pointer or function call addresses.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.72

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Buffer overflows are one of 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)	0.83

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 30

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

Question:

Explain six (6) aspects of Windows security mechanisms as presented in the Windows Security lecture, covering the role of subjects and tokens, the purpose of Active Directory, the nature of Windows access control, and the risks arising from the complexity of these mechanisms.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify what Windows treats as subjects, namely 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
2	State where the security credentials of a subject are kept, i.e. in a token.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.67
3	Describe Active Directory as an LDAP-like directory service introduced in Windows 2000 for organising 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	Note that Windows systems provide complex mechanisms for user account and object management and for access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.83
5	Explain that DACS allow fine-grained access control over heterogeneous 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)	0.69
6	Warn that the complexity of Windows security mechanisms can itself cause severe security incidents through misconfiguration or implementation bugs.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::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: 041 - Windows Security, slide 11; 041 - Windows Security, slide 21; 041 - Windows Security, slide 6

PART A - QUESTION 4

A4a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

A biometric system performs its work in two broad stages. List the TWO (2) stages of the biometric authentication process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identification stage, in which the 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Authentication stage, in which acquisition is repeated and the result is compared and a decision made	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::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: 072 - Biometrics and Authentication, slide 5

A4b - 6 marks - supported by lecture slides (not lecturer-marked)

Question:

Refer to your answer in (a). Discuss biometric mechanisms and technologies as an alternative to passwords, covering the definition of a biometric, the two categories of biometric applications, and the specific technologies with their limitations.

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 are categorized into two sectors: psychological and behavioural.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.71
3	The psychological 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)	0.78
4	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
5	Retinal scanning is very efficient and cannot be spoofed, but it has disadvantages such as the user having to look directly, a high FTE ratio, acceptability concerns, light exposure and hygiene.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 9 072 - Biometrics and Authentication::s09::1	partly supported	0.14 LOW
6	Fingerprint biometrics suffer from disadvantages including racial issues, dirt, grime and wounds, placement of finger, too big a database to process, and spoofing so liveness is important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	partly supported	0.16 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 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7; 072 - Biometrics and Authentication, slide 9

PART A - QUESTION 5**A5a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

State TWO (2) password security controls that can be applied to protect password files and accounts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Applying access control to password files	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.80
2	Deactivating accounts after multiple 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)	0.71

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

Citations: 022 - Identification and Authentication, slide 12

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

State SIX (6) facts about Kerberos and single sign-on (SSO) as authentication mechanisms, covering the motivation for SSO, the design criteria of Kerberos, and the strengths and weaknesses of Kerberos.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	One motivation for single sign-on is to reduce the number of passwords users must memorize.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.33 LOW
2	Single sign-on can be implemented through client-server architectures such as Kerberos or 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
3	Kerberos is designed to resist eavesdropping by never transmitting passwords in clear text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported	0.44 LOW
4	Kerberos is designed for transparency, 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
5	Kerberos provides secure authentication even over an insecure network.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 23 022 - Identification and Authentication::s23::1	supported (stem gate)	0.62

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	A weakness of Kerberos is that it constitutes a single point of failure.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 23 022 - Identification and Authentication::s23::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: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 23

PART A - QUESTION 6

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

Question:

Explain two characteristics of Trojan horse malware as described in the lecture, focusing on how it behaves and what it does to the host system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans disguise themselves as useful or benign software so that users install them unsuspectingly.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Once running, a Trojan steals private data, deletes files, records keystrokes, or creates a way for further malware to be installed.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::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: 051 - Software Security, slide 12

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

Question:

Discuss six malware attack techniques and propagation methods described in the lecture, explaining for each how the technique operates and what impact it has on the infected system or its users.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Rootkits conceal malicious processes and software on the infected machine so that the attacker retains privileged remote access.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.67
2	Rootkits are typically installed after a vulnerability has been discovered, allowing the attacker to keep control of the compromised computer.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported	0.46 LOW
3	Spyware gathers sensitive user data such as logins, passwords, visited sites and keystrokes, and can redirect the browser to unwanted sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.60
4	An executable-file virus can propagate by appending its virus body to a host program.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported	0.44 LOW
5	An executable-file virus can hijack execution by overwriting the 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)	0.55

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	The Morris worm propagated across the Arpanet by exploiting a debugging feature of sendmail that allowed remote execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly 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:

List the four goals of access control and state what a reference monitor does in an access control system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The four goals of access control are 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)	1.00
2	A reference monitor is the instrument that makes authorization decisions and realizes access control policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.50

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: 023 - Access Control and Authorization, slide 4

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

Question:

Describe the Chinese Wall model by stating the concern it is designed to address, explaining its simple security rule and its write-access rule, and explaining how a subject's permitted access changes over time.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall policy is intended to resolve 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)	0.71
2	It is classified as a confidentiality access control policy rather than an integrity policy.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.62
3	Under the simple security rule, access is granted only if the object lies within the Wall or in a completely different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	partly supported	0.20 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	The write rule allows a write only if the simple security rule permits it and no object readable by the subject lies in a different company dataset containing unsanitized information.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	supported (stem gate)	0.75
5	Access rights are dynamic and depend on the subject's history of previous accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.86
6	Once a subject accesses one company's information, it is blocked from companies in the same conflict class but remains free to access companies in other conflict classes.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	partly supported	0.15 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: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 24; 024 - Formal Security Model, slide 25; 024 - Formal Security Model, slide 26

PART A - QUESTION 8

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

Question:

Explain how a disclosure threat and a usurpation threat each affect the confidentiality, integrity and availability of a system's assets.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A disclosure threat involves unauthorized access to information, which breaches confidentiality, and confidentiality services are the countermeasure against it.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.36 LOW
2	A usurpation threat is unauthorized control of part of a system, and availability services are what counter this threat.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::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: 011 - Introduction to Computer Security, slide 10

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

Question:

State six facts about the Samy worm and the cross-site scripting (XSS) behaviour it exploited, covering how the malicious script was injected, how it spread between users, 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 manipulating 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	The worm retrieved 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
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 own profile and friends list infected with the JavaScript and with Samy.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.73
5	The incident eventually infected 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 underlying XSS weakness 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

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 15

PART A - QUESTION 9

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

Question:

Explain how NIDS sensors should be positioned in a network and give one typical location for such a sensor.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors should be placed strategically 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)	0.88
2	A typical sensor location is just inside the firewall (or on the DMZ, server farm segment, or segment connecting mainframe/midrange hosts).	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.21 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

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

Question:

Describe six preventive network security mechanisms and, for each, state the protection it provides to an organization's 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 acts as a firewall and web filter to improve data security and network performance.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.73

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
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 limits each user to only the access and permission 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 10

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

Question:

Explain two advantages that adopting an organisational code of ethics brings to a computing professional's conduct, and state what may happen to a member who fails to follow such a code.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	It makes acceptable standards of behaviour clearer to understand.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported (stem gate)	0.50
2	It communicates shared guidelines that everyone is expected to follow.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported (stem gate)	0.67

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 8

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

Question:

Discuss the ethical responsibilities of computing professionals and organisations in protecting the privacy of users' personal information, with reference to professional codes of ethics and the constraints under which information specialists must operate.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Computing professionals are expected to follow a formal code of ethics and professional conduct, such as that of the ACM.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.60

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Professional bodies such as AITP support members with education and information on relevant IT issues, helping them handle privacy concerns responsibly.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.31 LOW
3	The ACM maintains a code of ethics and professional conduct for computing professionals.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.86
4	Merely describing moral and ethical dimensions of ICT is insufficient; organisations must actively address privacy obligations.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.33 LOW
5	Users and especially information specialists have definite responsibilities to perform within ethical, moral and legal constraints, including protecting privacy.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.75
6	Organisations must ensure that privacy protection is treated as part of the ethical and legal constraints under which ICT is used.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.25 LOW

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 3; 071 - Ethics and Computer Security, slide 7

PART B - QUESTION 1

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

Question:

State the role of the TPM in a chain of trust, how the chain is built from hardware to software, and how the platform's trusted state is finally established.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The TPM is a tamper-resistant hardware module mounted in the platform that performs measurement, protected storage, integrity reporting and policy enforcement.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 6 073 - Trusted Computing::s06::1	partly supported	0.47 LOW
2	In the chain of trust, each stage measures and validates the next stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.67
3	The measurement results are recorded in Platform Configuration Registers (PCRs) located on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.67
4	The chain begins at the hardware TPM and then proceeds through software components such as the RTM, TPM software stack, BIOS and kernel.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.39 LOW
5	At the end of the chain, the whole platform is verified to be in a trusted state.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.67

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 6; 073 - Trusted Computing, slide 8

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

Question:

Discuss the NGSCB/Nexus architecture by describing its two primary system components and the security functions each performs on the trusted platform.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is described as a special kernel forming 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	Nexus isolates normal-mode processes from trusted-mode processes by separating 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	Nexus authenticates and protects data that is entered, stored, communicated and displayed by means of encryption.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.80
4	The Nexus security kernel is authenticated at boot, authenticates trusted programs, and provides the application interface to the TPM without trusting the OS.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.33 LOW
5	The Nexus Computing Agent is a trusted software component that runs in trusted mode and communicates with 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 B - QUESTION 2

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

Question:

Explain five ways in which intrusion detection systems and related protection mechanisms are used to detect and defend against attacks on computer systems.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS detects malicious activity occurring in computer systems.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported (stem gate)	0.71
2	An IDS can identify and stop an attack while it is still in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported	0.43 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	An IDS supports 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	0.38 LOW
4	A passive detection system can only log and alert when an attack is identified.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 29 062 - Intrusion Detection System::s29::1	supported (stem gate)	0.67
5	A passive detection system is unable to actively stop an attack that is in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 29 062 - Intrusion Detection System::s29::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: 062 - Intrusion Detection System, slide 2; 062 - Intrusion Detection System, slide 29

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

Question:

Explain five threat classes and countermeasures described in the lecture, covering how threats are defined, how attacks relate to vulnerabilities, and how protection mechanisms and specific defences address these dangers.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A threat is defined as an entity that represents a constant danger to an asset.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported (stem gate)	0.86
2	An attack is described as a deliberate act that takes advantage of a vulnerability.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported (stem gate)	0.67
3	Protection of assets involves prevention, detection and response techniques.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 28 011 - Introduction to Computer Security::s28::1	supported (stem gate)	0.86
4	Threats are potential violations of security, whereas attacks are actual violations.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	0.57
5	Sandboxing provides a safe, isolated environment for running or opening suspected insecure programs or files.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 26 061 - Network Security::s26::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: 011 - Introduction to Computer Security, slide 28; 011 - Introduction to Computer Security, slide 9; 061 - Network Security, slide 26

