



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:

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 disguise themselves as useful or benign software in order to be run by the user.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Once active, a Trojan steals private data, deletes files, logs keystrokes or opens a way for additional malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.64

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

Citations: 051 - Software Security, slide 12

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

Question:

Explain six (6) techniques by which malware infects host programs or propagates across systems, as described in the lecture material on software security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can infect a COM executable by appending its virus body to the host program.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported	0.44 LOW
2	The virus saves the original program entry point inside its own virus body before taking control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.50
3	The program entry point is replaced with a jump into the virus body so the virus executes first.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.70
4	For EXE files, the virus overwrites the program header so that the entry point is switched to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.67
5	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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	The Brain virus spread in the wild by being included in the boot sector of distributed software diskettes.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::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 10; 051 - Software Security, slide 7; 051 - Software Security, slide 9

PART A - QUESTION 2

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

Question:

List two ways in which morals, ethics and laws differ from one another as 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 within a society.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.67
2	Laws are formal rules of conduct imposed by a sovereign authority such as a government on its citizens.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	1.00

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

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

Citations: 071 - Ethics and Computer Security, slide 5

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

Question:

Refer to your answer in (a). Discuss how a professional code of ethics and conduct guides a computing professional's behaviour, using the ACM code as your example. Your discussion should cover six distinct requirements of such a code.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that 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	Note that the ACM is a professional body that has established 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)	0.67
3	Explain that the code obliges 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)	0.64

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Explain that the code requires the professional to respect privacy and to 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	0.29 LOW
5	Explain that the code requires the professional to strive for high quality in the processes and products of professional work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.78
6	Explain that the code requires the professional to give thorough evaluations of computer systems and their impacts, including 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)	0.73

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 3

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

Question:

Explain the Chinese Wall model as a formal security model, stating the concern it is designed to address and how its access decisions differ from static policies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall policy is intended to address conflicts of interest affecting 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)	0.80
2	Access rights under this policy are not static but depend on the subject's history of past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.55

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

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

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

Question:

Describe six aspects of access control structures, covering the access control matrix, access control lists and capabilities, including the advantages and disadvantages of the matrix and of ACLs.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that an access control matrix is a fundamental access control structure.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.40 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Give clarity of definition as an advantage of the access control matrix.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported	0.33 LOW
3	Give poor scalability as a disadvantage of the access control matrix.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	supported (stem gate)	0.50
4	Explain that an ACL describes access rights from the perspective of the 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)	0.80
5	Identify difficulty of revocation as a drawback of ACLs.	[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
6	Name capabilities (C-List) 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	0.40 LOW

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

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

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

PART A - QUESTION 4

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

Question:

Explain how the classes of threats described in the lecture affect the confidentiality, integrity and availability of information assets.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure threats such as snooping, sniffing and wiretapping breach confidentiality, which confidentiality services are meant to counter.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.09 LOW
2	Deception and disruption threats involve modification of data, so integrity services are the countermeasure for these threats.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.33 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

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

Question:

State SIX (6) facts about the Samy worm and the cross-site scripting (XSS) attack it exploited, covering how the malicious script was injected, how it spread to other users, and why unfiltered user input enables such attacks.

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 the 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 and with Samy.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.80
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	Any web application that returns user input without filtering is a potential XSS vulnerability.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.91

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 5

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

Question:

Explain what a buffer overflow is and how it can be exploited, referring to the behaviour of strcpy() and the effect on the stack.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	strcpy() copies the input string without verifying its length, so a longer string than the destination buffer causes an overflow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	partly supported	0.23 LOW
2	Because no bound checking is performed, the overflowing buffer content spills into the adjacent higher stack area.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.61

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

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

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

Question:

Describe six Windows security mechanisms and features, covering how user accounts and objects are managed, how access control is applied, how subjects obtain credentials, what Active Directory organises, how access rights are encoded, 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 includes elaborate mechanisms for managing user accounts and objects and for controlling access.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.80
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 can backfire, since misconfiguration and implementation bugs can cause serious incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.46 LOW
4	In Windows, processes and threads act as the active subjects of the operating system.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	supported (stem gate)	0.50
5	A subject's security credentials are kept in a token, which maps principals to subjects 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	Active Directory, introduced with Windows 2000, is an LDAP-like directory service used to organise users and groups, credentials and certificates, resources, policies, DNS and trust.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.53

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 21; 041 - Windows Security, slide 6

PART A - QUESTION 6**A6a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

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

Marking points:

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

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

Discuss biometric technologies by categorising the types of biometric applications available today and, for each category, giving examples. Then discuss two disadvantages associated with specific biometric technologies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Biometric applications are divided into two sectors, namely 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)	0.57
2	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
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	Fingerprint biometrics suffer from racial issues, dirt, grime and wounds, and placement of the finger.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	supported (stem gate)	0.70
5	Fingerprints can be spoofed, so liveness detection is important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	supported (stem gate)	0.67
6	Retinal scanning raises acceptability concerns relating to light exposure and hygiene.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 9 072 - Biometrics and Authentication::s09::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: 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7; 072 - Biometrics and Authentication, slide 9

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

State TWO (2) limitations of misuse detection systems when used to detect attacks.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Misuse detection systems are ineffective against previously unknown attack methods.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 17 062 - Intrusion Detection System::s17::1	supported	0.44 LOW
2	State transition analysis cannot detect denial of service attacks.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 21 062 - Intrusion Detection System::s21::1	supported	0.43 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 17; 062 - Intrusion Detection System, slide 21

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

Question:

A security analyst is preparing a briefing on malware threat classes and the countermeasures that address them. Explain the threat posed by rootkits, spyware and adware, and the countermeasures or defensive considerations associated with each.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Rootkits conceal malicious processes and software on the infected system so that privileged remote access can be maintained.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.75
2	Rootkits are typically installed after a vulnerability has been found and exploited, keeping the machine under the attacker's control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.54
3	Detecting rootkits is difficult because they are designed to hide from the very detection software used against them.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.73
4	Spyware steals user credentials and records activity such as sites visited 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)	0.57
5	The impact of spyware includes identity theft and compromise of sensitive banking information.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.67
6	Adware is largely harmless but annoying, generating pop-up advertisements that interrupt other programs.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.64

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

Citations: 051 - Software Security, slide 13

PART A - QUESTION 8

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

Question:

Explain how the chain of trust works 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
-----	----------------	----------------	--------	---------	---------

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the chain measures and validates the following stage, with the resulting measurements 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	0.25 LOW
2	The chain begins at the hardware TPM and proceeds through the software stages (RTM, TPM Software Stack, BIOS, kernel), so that the whole platform ends up verified as trusted.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.23 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

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

Question:

Compare the two primary system components of the Next Generation Secure Computing Base, namely the Nexus and the Nexus Computing Agent, in terms of their roles and characteristics. Provide six distinct points of comparison.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Nexus is described as 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 aims to isolate normal-mode processes from trusted-mode processes differently in memory.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.75
3	The Nexus provides functionality to authenticate and protect 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)	0.75
4	The Nexus acts as 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)	0.67
5	The Nexus authenticates trusted programs and serves as the application interface to the TPM, while not trusting the OS.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.30 LOW
6	The Nexus Computing Agent is a trusted software component that runs in trusted mode and communicates with the Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported (stem gate)	0.75

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

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

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

PART A - QUESTION 9

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

Question:

Explain two password security controls that can be applied to password files and accounts in order to

strengthen password-based authentication.

Marking points:

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

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

Citations: 022 - Identification and Authentication, slide 12

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

Question:

Explain the mechanisms of Kerberos, smartcards and single sign-on as alternative authentication approaches, covering the motivation for single sign-on, the categories of single sign-on solutions, how a Kerberos user login establishes a secret key, and the role of smartcards.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the need for users to memorize passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.57
2	Single sign-on reduces the time spent typing passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.67
3	Single sign-on solutions include local password containers such as KDE Wallet.	[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 can be implemented 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
5	In Kerberos login, the hash of the user's password becomes the secret key of the client/user.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.75

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	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.

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

PART A - QUESTION 10

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

Question:

A network administrator is deploying a Network-Based Intrusion Detection System (NIDS) to protect an organization's critical servers. List TWO (2) typical locations where NIDS sensors should be placed.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensor placement 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)	0.60
2	Sensor placement on the DMZ	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported	0.33 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

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

Question:

A company wants to strengthen its network defences before deploying monitoring tools. State SIX (6) preventive network security mechanisms and, for each, briefly describe what it does.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Firewall: filters inbound and outbound network traffic according to predefined security rules.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported	0.30 LOW
2	Proxy server: improves data security and network performance, acting as a firewall and web filter while caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.69
3	Network segmentation: creates boundaries between network 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	Remote access VPN: gives individual hosts or clients secure remote access to the organization network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	Zero Trust Network Access: restricts each user to only the access and permissions needed for their role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.50

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	IDS/IPS: detects or prevents 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.

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

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 ways in which a voluntary professional code of ethics can shape the ethical impact of the technology that computing professionals build and deploy, and note the limits of relying on such a code.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A code may fail to represent the ethical views of every individual in the group it covers.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.40 LOW
2	Such a code is frequently not enforceable against members.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.14 LOW
3	It functions as a code of conduct rather than a legal instrument.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.43 LOW
4	Merely describing ethical dimensions of ICT is insufficient; the code must prescribe expected behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.30 LOW
5	It reminds users and information specialists that they have definite duties to act within ethical, moral and legal limits.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.64

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

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

Citations: 071 - Ethics and Computer Security, slide 3; 071 - Ethics and Computer Security, slide 9

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

Question:

Using the hospital scenario, explain five ethical concerns that the programmer should raise with management regarding the privacy of patients' information and the organization's responsibility for it.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The organization must safeguard patients' personal information as a matter of privacy.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	partly supported	0.25 LOW
2	The organization must ensure that stored patient data is accurate and can be verified as genuine.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	partly supported	0.00 LOW
3	The organization must decide who owns the patient information and under what conditions it may be sold or exchanged.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported	0.42 LOW
4	The organization must define which staff have a right to obtain information about patients and how that information may be used.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported	0.36 LOW
5	The organization should recognize that without law and justice, conduct such as unauthorized snooping makes people behave in the worst possible way.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 4 071 - Ethics and Computer Security::s04::1	partly supported	0.19 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: 071 - Ethics and Computer Security, slide 13; 071 - Ethics and Computer Security, slide 4

PART B - QUESTION 2

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

Question:

Discuss the goals of access control and the role of a reference monitor in making authorization decisions, then explain how the Chinese Wall model constrains access through its simple security rule and its write property.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control aims to grant access to subjects.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.60
2	Access control also aims to limit access.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported	0.40 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	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
4	The Chinese Wall simple security rule permits a subject access to an object only when that object is either within the subject's existing wall (the same company datasets already accessed) or belongs to 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	supported (stem gate)	0.52
5	The Chinese Wall write property permits write access only when the simple security rule allows it and no readable object in a different company dataset contains unsanitized information.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	partly supported	0.21 LOW

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

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

Citations: 023 - Access Control and Authorization, slide 4; 024 - Formal Security Model, slide 25; 024 - Formal Security Model, slide 26

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

Question:

State five key security models and, for each, the distinguishing feature given in the lecture, including the model that identifies conflicts of interest and the model that adds integrity verification.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula (BLP) model is listed as a key security model concerned with access control only.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.78
2	The Biba model is listed as a key security model that performs additional integrity verification.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.71
3	The Chinese Wall model is listed as a key security model for identification of 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)	0.86
4	The Take-grant model is listed as a key security model giving a graph-theoretical interpretation of an access matrix.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.89
5	The Chinese Wall policy, proposed by Brewer and Nash in 1989, is described as addressing 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)	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 21; 024 - Formal Security Model, slide 5

End of marking scheme.