



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 forms of guidance for professional conduct in computer security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct, 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 requirements that a professional code of ethics and conduct, such as the ACM code, places on a computing professional's behaviour in security-related work.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The professional must aim for high quality in the processes and products of their 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)	0.75
2	The professional must uphold strong levels 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)	0.56

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The professional must be aware of and comply with existing rules that govern 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)	0.50
4	The professional must only carry out work within the areas in which they are competent.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported	0.40 LOW
5	The professional must contribute to society and human well-being, recognising all people as stakeholders in computing.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.73
6	The professional must treat privacy as something to be respected in their work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.29 LOW

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

PART A - QUESTION 2

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

Question:

List two characteristics of Trojan horses as a type of malware, based on how they behave and what they do to the host system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans disguise themselves as useful or benign programs so that users accept them.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.12 LOW
2	Once running, trojans steal private data, delete files, log keystrokes or open 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)	0.71

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

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

Citations: 051 - Software Security, slide 12

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

Question:

Discuss six techniques by which malware attacks and propagates through computer systems, covering how malicious code is inserted into executables, how early viruses and worms spread, and how rootkits and spyware operate on infected hosts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can be attached to an executable by appending the virus body to the program.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.57

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	An executable can be infected by overwriting its header so that the entry point is redirected to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported	0.44 LOW
3	Early malware such as Elk Cloner spread by infecting the boot sector.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.44 LOW
4	The Morris worm propagated across the Arpanet by exploiting a debugging feature of sendmail for remote execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.40 LOW
5	A rootkit hides malicious processes and software in the infected system so that privileged remote access is maintained.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.82
6	Spyware spies on users by stealing logins and passwords, logging keystrokes and redirecting browsers to unwanted sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::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 10; 051 - Software Security, slide 13; 051 - Software Security, slide 7

PART A - QUESTION 3

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

Question:

List TWO (2) reasons why software is insecure, with particular reference to buffer overflows.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Attackers can cause insecurity by altering resources that are essential to 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)	0.67
2	A major cause of software insecurity is the failure to validate input supplied by users.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::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: 051 - Software Security, slide 30

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

Question:

State six (6) security mechanisms and components that Windows provides for managing users, controlling access and enforcing privileges, and note how the complexity of these mechanisms can itself become a security risk.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows includes a Security Reference Monitor operating in kernel mode that performs ACL verification.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	partly supported	0.36 LOW
2	The Local Security Authority handles password verification and change, access tokens and audit logs.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.82

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The Security Accounts Manager maintains the accounts database and performs password encryption.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.75
4	User Account Control, introduced in Vista, enforces limited user privileges.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.88
5	Active Directory, introduced in Windows 2000, is an LDAP-like directory service used to organize system resources such as users, groups, credentials and policies.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.69
6	The very complexity of Windows security mechanisms is a weakness, since misconfiguration and implementation bugs can cause severe security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.57

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 21; 041 - Windows Security, slide 3; 041 - Windows Security, slide 6

PART A - QUESTION 4

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

Question:

State two impacts of malware attacks on the confidentiality, integrity or availability of a system's data and services.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Malware can cause unauthorized disclosure of information, which is a breach of confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported	0.38 LOW
2	Malware can compromise integrity by modifying data without authorization.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.12 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:

Describe the Samy worm as a case study of a cross-site scripting (XSS) attack, covering how the malicious script was injected, how it spread, and the outcome of the incident.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by writing to the page body using document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.64
2	It obtained the list of a user's heroes by issuing a GET request on a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.43 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	It added Samy as a friend by performing an XML-HTTP request 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 visitor to an infected user's page had their own profile and friends list infected, so the worm spread from page to page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.46 LOW
5	The incident ultimately infected around one million MySpace profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.29 LOW
6	The root cause is that any web application returning 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)	0.77

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:

State TWO (2) formal security models that are listed as key security models, and for each, state the specific security concern it addresses.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Biba model is identified as a key security model that 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	partly supported	0.44 LOW
2	The Chinese Wall model is identified as a key security model aimed at 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)	0.71

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

Citations: 024 - Formal Security Model, slide 5

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

Question:

Refer to your answer in (a). Explain how the access control matrix, access control lists and capabilities each implement access policies, and state one advantage and one disadvantage of the matrix and of the list structure.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	The matrix offers clarity of definition as an advantage.	[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
3	The matrix suffers from 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	supported (stem gate)	0.67
4	An ACL is an object-centred description of access rights, illustrated by entries such as bill.doc granting Bob read and write.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	partly supported	0.33 LOW
5	The ACL gives easy access to an object's access rights and is relatively easy to manage using 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)	0.88
6	The ACL's drawbacks include a poor overview of rights per subject, difficulty of revocation and difficulty of sharing.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.64

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 6

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

Question:

State TWO (2) ways in which an intrusion detection system supports the detection and defence of a system against attacks.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The IDS confirms whether an attack succeeded or failed by examining host-based IDS log entries.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported	0.27 LOW
2	The IDS provides detection and response to attacks in near real time.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 14 062 - Intrusion Detection System::s14::1	supported (stem gate)	0.62

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

the public build.

Citations: 062 - Intrusion Detection System, slide 14

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

Question:

Compare how a misuse detection system and an anomaly detection system each classify activity as an attack, and explain one limitation of each approach when used as a countermeasure against threats.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Misuse detection represents attacks as patterns or signatures so that variations of the same attack can be recognised.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 17 062 - Intrusion Detection System::s17::1	supported (stem gate)	0.80
2	Misuse detection recognises known bad behaviour rather than unknown behaviour.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 17 062 - Intrusion Detection System::s17::1	supported	0.22 LOW
3	A limitation of misuse detection is that it is of little use against unknown attack methods.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 17 062 - Intrusion Detection System::s17::1	supported (stem gate)	0.62
4	Anomaly detection predicts future events from events that have already occurred using rules.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 25 062 - Intrusion Detection System::s25::1	supported (stem gate)	0.67
5	A limitation of anomaly detection is that intrusion scenarios not described by the rules will not be flagged.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 25 062 - Intrusion Detection System::s25::1	supported (stem gate)	0.56
6	An advantage of anomaly detection is that systems built on this model are highly adaptive to changes.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 25 062 - Intrusion Detection System::s25::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: 062 - Intrusion Detection System, slide 17; 062 - Intrusion Detection System, slide 25

PART A - QUESTION 7

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

Question:

Explain the goals of access control and the role of a reference monitor in realizing access control policies.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control aims to grant, limit, prevent and revoke access.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.86

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	A reference monitor is the instrument used to realize access control policies and can be deployed at all levels of the system hierarchy.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	0.54

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

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

Question:

*State the Chinese Wall policy and explain its simple security rule and its *-property. Then explain why this policy is described as addressing a specialised concern and how its permissions differ from static access rights.*

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Chinese Wall policy was proposed by Brewer and Nash to address 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
2	It is an access control confidentiality 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)	0.71
3	Under the simple security rule, a subject may access an object only if it is within the Wall (same company datasets already accessed) or in an entirely different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	partly supported	0.42 LOW
4	The *-property permits a write only when the simple security rule also allows the access and the subject cannot read any unsanitized object belonging to a different company dataset than the one being written to.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	supported (stem gate)	0.59
5	The policy is designed for a very specific concern: conflicts of interest faced 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)	0.89
6	Permissions change dynamically, since access rights depend on the 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)	0.89

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: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 24; 024 - Formal Security Model, slide 25; 024 - Formal Security Model, slide 26; 024 - Formal Security Model, slide 27

PART A - QUESTION 8

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

Explain the two stages of the biometric authentication process and state what activities occur in each stage.

Marking points:

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

Citations: 072 - Biometrics and Authentication, slide 5

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

Biometric technologies are grouped into different categories and each technology has its own operational characteristics. Explain the categories of biometric applications and the characteristics of iris and fingerprint 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	Iris scanning works by scanning the unique pattern of the iris.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	supported (stem gate)	0.80
5	Iris scanning requires no physical touch and overcomes the issues associated with retinal scanners.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.20 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Fingerprint authentication suffers from disadvantages such as 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	partly supported	0.17 LOW

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

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

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 to protect against unauthorised access.

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 block repeated guessing.	[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:

Describe six aspects of Kerberos and single sign-on mechanisms, covering the motivation for single sign-on, the design criteria of Kerberos, and how a user logs in to Kerberos.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the burden of remembering many passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.29 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Kerberos is designed to be secure against eavesdropping by never sending passwords in clear text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.60
4	Kerberos is designed for transparency, so the user is unaware of 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)	0.67
5	Kerberos is designed to be scalable, supporting many servers and clients.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.57
6	At login the user enters a user name and password at the client workstation.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::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: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 19

PART A - QUESTION 10

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

Question:

Explain how IDS sensors should be positioned in a network-based intrusion detection architecture, and give one typical location for such a sensor.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors must be placed 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)	0.75
2	A typical sensor location is just inside the firewall (or on the DMZ, the server farm segment, or segments connecting mainframe or 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

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

Question:

Explain three preventive network security mechanisms that an organization can deploy to protect its network, describing for each mechanism how it controls or secures network traffic.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall controls incoming and outgoing network traffic according to predetermined security policies.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
2	A proxy server improves data security and network performance by acting as a firewall and web filter, providing shared connections and caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.80
3	Network segmentation places boundaries between network segments whose computing assets share a common function, risk or role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.77
4	A remote access VPN gives individual hosts or clients remote and secure access to the organization's network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	Zero Trust Network Access restricts a user to only the access and permissions required to fulfill the role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.64
6	IDS/IPS mechanisms detect or prevent network attacks such as brute force attacks, denial-of-service attacks and exploits of network vulnerabilities.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.79

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

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

PART B - QUESTION 1

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

Scenario:

A hospital is deploying a fleet of networked medical workstations and wants each machine to prove, at boot time, that only approved software is running before it is allowed onto the clinical network. The security team proposes basing this assurance on a hardware module fitted to every workstation.

Question:

Discuss how a Trusted Platform Module and a chain of trust can be used to establish that a platform is in a trusted state, referring in your answer to the roots of trust and to the role of the TPM in the boot process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State the core principle of the Trusted Computing architecture, namely that each stage of the platform measures and validates the following stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported	0.30 LOW
2	Explain that the measurements produced during boot are recorded in Platform Configuration Registers held on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.50
3	Identify the sequence in which the chain proceeds, beginning with the hardware TPM and continuing through the RTM, the TPM software stack, the BIOS and the kernel.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.31 LOW
4	Describe the TPM as 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Explain the Root of Trust for Measurement as the component relied upon to measure and report to the Root of Trust for Reporting which software executes at the start of boot.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 7 073 - Trusted Computing::s07::1	supported (stem gate)	0.80

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 7; 073 - Trusted Computing, slide 8

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

Question:

In the hospital workstation deployment described in the scenario, the vendor proposes using the Next Generation Secure Computing Base rather than relying on the ordinary operating system. Explain the two primary system components of NGSCB and the role each plays in protecting the trusted mode of the workstation.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify that NGSCB's two primary components are the Nexus (a special security kernel that authenticates and protects data) and the Nexus Computing Agent (NCA).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	partly supported	0.27 LOW
2	Describe Nexus 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
3	Explain that Nexus is a security kernel that is authenticated on boot and that authenticates trusted programs.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.57
4	Note that Nexus provides the application interface to the TPM and does not trust the OS.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.33 LOW
5	Describe the Nexus Computing Agent as 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)

Scenario:

A software house is drafting a code of ethics for its security team. A junior analyst asks why the team should adopt a documented code at all, and a manager warns that the code may not bind every member and may be hard to enforce.

Question:

Explain five points about the ethical impact of adopting a documented code of ethics for a professional computing group, covering what such a code is, how it is established, what it does, and the limitations that reduce its ethical impact.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that a code of ethics is a written record of the behaviours a professional or social group considers acceptable.	[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
2	Note that the ethical standards in the code are set by the group itself rather than imposed from outside.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.09 LOW
3	Explain that the code classifies particular behaviours as either acceptable or unacceptable.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported	0.00 LOW
4	Point out that a code may fail to capture the personal ethics held by some individuals within the group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported	0.23 LOW
5	Observe that the code often cannot be enforced because it is a conduct code and not 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 (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: 071 - Ethics and Computer Security, slide 6; 071 - Ethics and Computer Security, slide 9

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

Question:

Referring to the scenario, state five points about the privacy responsibilities that a documented code of ethics places on the security team and the organisation, including the duties of individual specialists and the role of professional bodies' codes.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Information specialists, not only general users, carry definite responsibilities to act within ethical, moral and legal constraints, which includes handling private data appropriately.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.55
2	Merely describing moral and ethical dimensions of ICT is insufficient; the team must actively address privacy concerns rather than only documenting them.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.23 LOW
3	The organisation can adopt a recognised professional body's code, such as the ACM code of ethics and professional conduct, as the basis for its privacy obligations.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.36 LOW
4	Professional bodies such as AITP support members through education and information on relevant IT issues, helping the team understand its privacy duties.	[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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	The ACM maintains a code of ethics and professional conduct that the security team can follow when handling information responsibly.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	partly supported	0.36 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: 071 - Ethics and Computer Security, slide 3; 071 - Ethics and Computer Security, slide 7

End of marking scheme.