



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: 22 slots. Placeholders: 2.
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 14 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, 22 supported by lecture slides, 2 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 where network-based IDS sensors should be placed in a network and why their placement matters.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Sensors should be positioned at strategic points so that the most valuable assets are protected.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	supported (stem gate)	0.56
2	Typical sensor locations include just inside the firewall, on the DMZ, on the server farm segment, and on 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	partly supported	0.20 LOW

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

Citations: 062 - Intrusion Detection System, slide 7

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

Question:

Describe six preventive network security mechanisms and, for each, state the specific protective role it plays in 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 improves data security and network performance by acting as a firewall and web filter, sharing connections and caching data.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.79
3	Network segmentation creates boundaries between 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 secure access to an 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Zero Trust Network Access restricts a user to only the access and permissions needed to fulfil their role.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.55
6	IDS/IPS detect or prevent network 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 2

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

Question:

List TWO (2) reasons why software is insecure, as discussed in the Software Security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Attackers can cause insecurity by altering system resources that are essential 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)	0.69
2	A major cause of software insecurity is the failure to properly 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)	0.50

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

Citations: 051 - Software Security, slide 30

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

Question:

State six (6) Windows security mechanisms or components, as discussed in the Windows Security lecture, and briefly indicate the role of each.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Security Reference Monitor operating in kernel mode performs ACL verification.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	partly supported	0.44 LOW
2	The winlogon process in user mode handles user logon.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.67
3	The Local Security Authority is responsible for 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
4	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
5	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
6	Active Directory, introduced in Windows 2000, is an LDAP-like directory service used to organize system resources.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::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: 041 - Windows Security, slide 3; 041 - Windows Security, slide 6

PART A - QUESTION 3

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

Question:

State TWO (2) characteristics of a Trojan horse as a type of malware.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans typically disguise themselves as useful or benign programs.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.17 LOW
2	Trojans steal private information or damage the host system.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::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: 051 - Software Security, slide 12

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

Question:

Discuss six (6) ways in which malware attacks and propagates, referring to historical malware examples, executable infection techniques, and the behaviour of rootkits and spyware.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Early malware such as Elk Cloner spread by infecting the boot sector of disks.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.40 LOW
2	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
3	An executable 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 (stem gate)	0.50
4	An executable virus can hijack execution by overwriting a program header to redirect the entry point to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.50
5	Rootkits hide malicious processes and software so that the attacker retains privileged remote access to the infected system.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.75
6	Spyware attacks users by stealing their logins and passwords and by logging keystrokes.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::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: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 7

PART A - QUESTION 4

A4a - 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	It is designed to address a very specific concern, namely 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)	0.89
2	Access decisions are sensitive to the history of past accesses, so permissions change dynamically rather than being fixed in advance.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported	0.33 LOW

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

A4b - 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 state the requirements that any such structure must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control structures are the mechanisms through which access policies are implemented, and the access control matrix, capabilities and access control lists are named as such structures.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.60
2	The access control matrix is described as the basic control structure, valued for clarity of definition and ease of verification.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	partly supported	0.30 LOW
3	The access control 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	partly supported	0.25 LOW
4	An access control list is an object-centred description of access rights, giving easy access to the rights on an object and relative ease of management through abstractions.	[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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Access control lists have the drawbacks of a poor overview of rights per subject and difficulty of revocation and sharing.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	partly supported	0.08 LOW
6	Any access control structure must be able to express control policies and must offer verifiability of correctness together with scalability and manageability.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	partly supported	0.21 LOW

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

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

PART A - QUESTION 5

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

Question:

List two goals of access control and state the instrument used to make authorization decisions.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The reference monitor is the instrument 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)	0.83
2	The reference monitor is the mechanism 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)	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: 023 - Access Control and Authorization, slide 4

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

Question:

Refer to your answer in (a). Discuss six distinct features of formal security models, covering the Bell-La Padula, Biba and Chinese Wall models, including what each model controls and how the Chinese Wall model's rules constrain read and write access.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula model is described as providing access control only, without the additional integrity verification found in Biba.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	partly supported	0.46 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	The Biba model is characterised as adding integrity verification on top of access control.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported	0.44 LOW
3	The Chinese Wall model is presented 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)	0.50
4	Under the Chinese Wall simple security rule, a subject may access an object only if it lies within the wall of already accessed company datasets or belongs to an entirely different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	partly supported	0.33 LOW
5	The Chinese Wall *-property restricts writes: a write is allowed only if the simple security rule permits it and no object readable by the subject belongs to a different company dataset and holds unsanitized information.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 26 024 - Formal Security Model::s26::1	supported (stem gate)	0.70
6	Access permissions in the Chinese Wall model change dynamically, since the rights a subject enjoys depend on the history of its past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.71

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: 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 5

PART A - QUESTION 6

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

Question:

Explain how a disclosure threat and a usurpation threat each cause harm to a system, stating which security objective is affected in each case.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is the unauthorized access to information (e.g. via snooping, sniffing or wiretapping), and this harm to confidentiality is countered by confidentiality services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.33 LOW
2	Usurpation is the unauthorized control of some part of a system, and the resulting harm to availability is countered by availability services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported (stem gate)	0.55

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

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

Question:

The Samy worm spread rapidly across MySpace by exploiting a cross-site scripting flaw. Explain six (6) aspects of this incident, covering the underlying XSS vulnerability, how the worm injected and propagated itself, and the scale of the resulting infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The root cause is that any web application returning user input without filtering is potentially vulnerable to XSS.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.77
2	XSS permits arbitrary JavaScript to be executed inside the victim 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
3	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
4	It retrieved the victim's list of 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
5	It added Samy as a friend by performing XML-HTTP requests against the addFriends page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.70
6	Any visitor to an infected profile had their own profile and friends list infected, and roughly 1,000,000 MySpace profiles were eventually infected.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	partly supported	0.36 LOW

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 7

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

Question:

Explain how the chain of trust works in Trusted Computing, referring to the role of the TPM and the stages that are measured and validated.

Marking points:

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 stored 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 then proceeds through software stages such as the RTM, TPM Software Stack, BIOS and 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	0.26 LOW

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

Citations: 073 - Trusted Computing, slide 8

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

Question:

Describe six (6) components and characteristics of the NGSCB/Nexus architecture, covering both the Nexus kernel and the Nexus Computing Agent, as presented in the Trusted Computing lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is described 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)	0.80
2	Nexus authenticates trusted programs.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.75
3	Nexus provides the application interface to the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.60
4	Nexus does not trust the operating system.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	supported (stem gate)	0.50
5	The Nexus Computing Agent is a trusted software component.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported	0.40 LOW
6	The NCA runs in a trusted mode that communicates with Nexus.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::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: 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 8

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

Question:

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

Marking points:

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

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

Question:

Discuss how a professional code of ethics and conduct, such as the ACM code, guides a computing professional in carrying out security-related work. Your discussion should cover six (6) distinct obligations or expectations that such a code places on the professional.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The professional is expected to design and build systems that are secure in a robust and usable manner.	[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
2	The professional should only use computing and communication resources when they are authorised to do so or when the public good requires it.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.58
3	The professional must give thorough assessments of computer systems and their impacts, including an analysis of possible risks.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 12 071 - Ethics and Computer Security::s12::1	supported (stem gate)	0.73
4	The professional is required to respect the privacy of others.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.40 LOW
5	The professional is required to honour confidentiality.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.25 LOW
6	The code is a documented set of acceptable behaviours defined by a professional group, which identifies particular actions as 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	0.42 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; 071 - Ethics and Computer Security, slide 6

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

Explain the stages involved in the biometric authentication process, distinguishing clearly between the identification stage and the authentication stage.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The identification stage begins with acquisition of the biometric sample.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported (stem gate)	0.50
2	During identification, master characteristics are created and stored for later use.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	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 5

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

Question:

Biometric technologies are grouped into different categories and each technology has its own operational strengths and weaknesses. Explain the categories of biometric applications and the characteristics of specific biometric technologies, giving six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Biometric applications are divided into two sectors, namely physiological 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	Physiological biometrics include iris, fingerprints, hand, retinal and face recognition.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.67
3	Behavioural biometrics include 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	A biometric is defined as a physiological or behavioural characteristic that can distinguish one person from another and can theoretically be used for identification or verification.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.91
5	Iris scanning reads the unique pattern of the iris, requires no touch, and overcomes the issues of retinal scanners.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly supported	0.36 LOW
6	Fingerprint biometrics suffer disadvantages such as racial issues, dirt, grime and wounds, finger placement problems, and spoofing, so liveness detection is important.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 7 072 - Biometrics and Authentication::s07::1	partly supported	0.18 LOW

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

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

PART A - QUESTION 10

A10a - 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 misuse detection cannot identify denial of service attacks.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 21 062 - Intrusion Detection System::s21::1	supported	0.38 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

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

Question:

State the distinction between a vulnerability, a threat and an attack as presented in the security fundamentals lecture, and state one countermeasure principle for protecting assets against such dangers.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A vulnerability is described as a weakness of a system that can be exploited to damage assets.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	1.00
2	A threat is characterised as a potential violation of security rather than an actual one.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	0.50
3	An attack is defined as the actual violation of security.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 9 011 - Introduction to Computer Security::s09::1	supported (stem gate)	0.80
4	A threat is any object, person or other 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)	0.90
5	An attack is a deliberate act that exploits 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)	1.00
6	Protection of assets should combine 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)	0.75

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 28; 011 - Introduction to Computer Security, slide 9

PART B - QUESTION 1

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

State FIVE (5) password security controls that can be applied to protect a system's password files and user accounts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Apply access control to the password files so that only authorised parties can read them.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported	0.36 LOW
2	De-activate an account after several failed login attempts.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.71
3	Show the time of the user's last login so anomalies can be noticed.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	partly supported	0.38 LOW
4	Enforce password policies, for example for the root password.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 12 022 - Identification and Authentication::s12::1	supported (stem gate)	0.60
5	Store the password in encrypted form using a one-way hash function.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 8 022 - Identification and Authentication::s08::1	supported (stem gate)	1.00

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

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

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

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

Explain the design criteria that Kerberos satisfies and the benefits that motivate organisations to adopt single sign-on solutions such as Kerberos, smart cards and two-factor authentication.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Kerberos prevents eavesdropping because no password is ever transmitted 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
2	Kerberos is transparent to the user, who 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Single sign-on reduces the burden of remembering and typing passwords and lowers password maintenance effort.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	partly supported	0.22 LOW
4	Single sign-on can be realised through client-server architectures such as Kerberos and Active Directory.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.50
5	Smart cards, biometrics and two-factor authentication are alternatives to passwords and shared secrets.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 24 022 - Identification and Authentication::s24::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: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 24

PART B - QUESTION 2

B2a - 5 marks - PLACEHOLDER

Topic: risk/management (ethics); command: Explain

Status: placeholder - no supported question passed verification.

Reason: B2a: near-duplicate (seq 0.69, content 0.65) of accepted A8b: 'Discuss how a professional code of ethics and conduct, such as the ACM code, guides a computing professional in carrying out security-relate'; choose a different question angle

B2b - 5 marks - PLACEHOLDER

Topic: risk/management (ethics); command: Discuss

Status: placeholder - no supported question passed verification.

Reason: B2b: Part B (a) is unresolved

End of marking scheme.