



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: 23 slots. Placeholders: 1.
Questions and answers are for local study use only.
5. Near-copy rejection used all 35 past papers; style widening is recorded per slot.

FOR MARKERS' USE ONLY

This marking scheme consists of 15 printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

Labels: computed / supported by lecture slides (not lecturer-marked) / placeholder. No official marking scheme exists for the real CSC662 papers; this is generated for the mock.

Entailment labels: supported = the private quote directly supports the point (or the point passed the stem-overlap gate); partly supported = partial/ambiguous support; not supported = no support. Quote text is omitted here; verdicts come from private verification.

Part A: $10 \times (2 + 6) = 80$ marks. Part B: $2 \times (5 + 5) = 20$ marks. Total: 100 marks. Slots: 0 computed, 23 supported by lecture slides, 1 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) facts about how a chain of trust is established in the Trusted Computing architecture, referring to the role of the TPM and the sequence of measured components.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the chain measures and validates the following stage.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	supported (stem gate)	0.60
2	The measurements produced during the chain are stored in Platform Configuration Registers on the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::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: 073 - Trusted Computing, slide 8

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

Question:

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is described as a special kernel forming the core of the trusted operating environment.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.62
2	Nexus isolates the normal mode process from the trusted mode process by handling them differently in memory.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.67
3	Nexus authenticates and protects data that is entered, stored, communicated and displayed by means of data encryption.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.80
4	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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Nexus provides the application interface to the TPM and does not trust the operating system.	[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 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.

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

PART A - QUESTION 2

A2a - 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 those master characteristics.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	supported	0.33 LOW
2	The authentication stage involves further acquisition(s), comparison of the presented sample, 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)	0.62

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

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

Question:

State six facts about biometric technologies used for authentication, covering the definition of a biometric, the two categories of biometric applications, and the specific technologies and their characteristics.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A biometric is defined as a physiological or behavioural characteristic of a human being that can distinguish one person from another.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.89
2	Biometric applications available today are divided into two sectors.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.86

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	The psychological sector includes iris, fingerprints, hand, retinal and face recognition.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.78
4	The behavioural sector includes voice, typing pattern and signature.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.67
5	Fingerprint processing divides the print into loops, whorls and arch and calculates minutiae points.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 6 072 - Biometrics and Authentication::s06::1	supported (stem gate)	0.55
6	Iris scanning reads the unique pattern of the iris, which is coloured and visible from far, and requires no touch.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 10 072 - Biometrics and Authentication::s10::1	partly 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: 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 6

PART A - QUESTION 3

A3a - 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

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

Question:

Explain the role of a professional code of ethics and conduct for computing professionals, referring to the ACM code and its professional conduct expectations.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Ethics is a documented set of acceptable behaviours for a professional or social group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.75
2	The code is defined by the group itself, so the profession sets its own standards.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	partly supported	0.25 LOW
3	The code identifies which specific actions are appropriate or inappropriate.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.75
4	The ACM, founded in 1947, has 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)	1.00
5	Under the ACM code, a professional should 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)	0.54
6	ACM professional conduct requires striving for high quality in both 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)	0.73

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 4**A4a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans typically disguise themselves as useful or benign software.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Trojans replicate themselves and steal 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)	0.88

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

Citations: 051 - Software Security, slide 12

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

State SIX (6) techniques by which malware propagates itself or conceals its activity within an infected system, as described in the software security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can attach its body to an existing program file so that the host program carries the malicious code.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported	0.27 LOW
2	The virus stores the original program entry point inside its own body so control can later return to the legitimate code.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported	0.33 LOW
3	The virus redirects execution by replacing the program entry point with a jump into the virus body.	[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	A rootkit hides malicious processes and software on the infected machine so that the attacker keeps privileged remote access.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.67
6	Spyware collects user credentials and activity, for example by logging keystrokes or recording visited sites.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported	0.46 LOW

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

Citations: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 9

PART A - QUESTION 5

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

Question:

Explain how a buffer overflow arises in a program such as the one using strcpy() into a fixed-size local buffer, and how an attacker can exploit it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The overflow occurs because strcpy() copies the input without checking its length against the buffer size.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.25 LOW
2	By controlling the overflowing buffer content, the attacker overwrites the return address and hijacks the execution flow.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::1	supported (stem gate)	0.82

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

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

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

Question:

Explain six security mechanisms and structures that Windows provides for managing user accounts, subjects and system resources, and note why the complexity of these mechanisms can itself become a security concern.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows offers elaborate built-in mechanisms covering user account management, object management and access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.67
2	Discretionary access control in Windows allows fine-grained control over diverse entities both in the OS and in applications.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.50
3	The same complexity is a liability, since misconfiguration or implementation bugs can cause serious security incidents.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported	0.42 LOW
4	Active Directory, introduced with Windows 2000, acts as an LDAP-like directory service organising system resources.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.83
5	Subjects in Windows are the active entities, namely processes and threads, whose security credentials are held in a token.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	partly supported	0.36 LOW
6	Tokens carry the security credentials for a subject and are inherited, possibly with restrictions, when new processes are created.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::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: 041 - Windows Security, slide 11; 041 - Windows Security, slide 21; 041 - Windows Security, slide 6

PART A - QUESTION 6

A6a - 2 marks - PLACEHOLDER

Topic: attacks/malware; command: List

Status: placeholder - no supported question passed verification.

Reason: A6a: sub-angle not followed; use one of ['confidentiality', 'integrity', 'availability', 'impact', 'harm', 'damage']

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

Question:

The Samy worm spread through MySpace by exploiting cross-site scripting. Describe the Samy worm case study by explaining how the worm injected itself, how it propagated to other users, and the scale of the resulting infection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile using document.body.innerHTML.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
2	The worm obtained the list of 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 friend 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 visitor to an infected user's page had their profile and friends list infected with Samy.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.67
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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	The underlying XSS weakness 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 7

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

Question:

List TWO (2) typical locations where IDS sensors are placed in a network-based IDS architecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor location 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	A sensor location 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

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

Question:

Refer to your answer in (a). Explain how preventive network security mechanisms, such as firewalls, proxy servers, network segmentation and remote access VPN, reduce the attacks that an IDS must later detect, and state the limitation of these preventive mechanisms.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall controls incoming and outgoing traffic on the network 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 remote and secure access to the organization network.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 4 061 - Network Security::s04::1	supported (stem gate)	0.89
5	These preventive mechanisms cannot stop every intrusion, so the IDS monitors network resources to detect intrusions and attacks that were not stopped by them.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 3 062 - Intrusion Detection System::s03::1	supported (stem gate)	0.64

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	The limitation is that preventive mechanisms alone are insufficient, so IDS/IPS is still needed to detect or prevent attacks such as brute force, denial-of-service 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)	0.58

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

Citations: 061 - Network Security, slide 3; 061 - Network Security, slide 4; 062 - Intrusion Detection System, slide 3

PART A - QUESTION 8

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

Question:

Explain two ways in which a professional code of ethics and conduct, such as the ACM code, guides the ethical conduct of computing professionals and shapes the ethical impact of the technology they build.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A code of ethics clarifies what counts as acceptable professional behaviour, making ethical standards easier to understand.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported	0.27 LOW
2	A code communicates shared guidelines that all members of the profession are expected to follow.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported	0.33 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 8

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

Question:

Compare morals and laws as forms of conduct guidance for computing professionals, and explain how organizational responsibility for privacy is reflected in professional conduct expectations such as those of the ACM code. Provide six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals and ethics are treated as distinct from merely describing behaviour, so a professional cannot rely on description alone when judging conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported	0.23 LOW
2	Computing professionals, and information specialists especially, carry definite duties to act within ethical constraints.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported	0.33 LOW
3	Users generally, not only specialists, are also bound by these responsibilities, showing that conduct guidance applies organization-wide.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported	0.29 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Laws are distinguished from morals because law and justice are presented as what keeps a person from becoming the worst of all, i.e. law is an external enforceable constraint.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 4 071 - Ethics and Computer Security::s04::1	partly supported	0.31 LOW
5	Morals concern the internal perfection of the person, since a perfected man is the best of animals, whereas law supplies the external justice that morals alone cannot guarantee.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 4 071 - Ethics and Computer Security::s04::1	partly supported	0.23 LOW
6	Organizational responsibility for privacy means the professional code frames conduct in terms of ethical, moral and legal constraints that the organization and its staff must satisfy.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.25 LOW

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

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 4

PART A - QUESTION 9

A9a - 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 handle 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)	0.70
2	Access decisions under the Chinese Wall depend on the subject's history of previous accesses, so permissions change dynamically.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::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 24; 024 - Formal Security Model, slide 27

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

Question:

Discuss six points about the access control matrix, access control lists and capabilities as access control structures, covering what each structure represents and the strengths or weaknesses of each.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that the access control matrix is regarded 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	0.38 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Give clarity of definition and ease of verification as advantages 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	0.25 LOW
3	Identify poor scalability and poor handling of changes as disadvantages 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)	0.62
4	Explain that an ACL describes access rights from the object's perspective, listing which subjects may access that object and how.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.57
5	Note that ACLs give easy access to an object's access rights and are relatively easy to manage through abstractions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.70
6	List poor overview of access rights per subject, difficulty of revocation and difficulty of sharing as ACL drawbacks.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.73

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 8

PART A - QUESTION 10

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

Question:

Explain two password security controls that can be applied to password files and user accounts to protect an authentication system.

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

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

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

Question:

Describe six facts about single sign-on and Kerberos as authentication mechanisms, covering the motivations for single sign-on, the categories of solutions, the design criteria of Kerberos, and how a user's password is used at login.

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 users spend typing passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.43 LOW
3	Single sign-on solutions include 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)	0.55
4	Kerberos is designed to be secure against eavesdropping by never transmitting passwords in clear text.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.60
5	Kerberos is designed for transparency, so the user is unaware of any authentication beyond the initial login.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.70
6	At 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

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 B - QUESTION 1**B1a - 5 marks - supported by lecture slides (not lecturer-marked)****Question:**

Discuss how intrusion detection systems support the detection of and defence against attacks on computer systems. In your answer, describe five distinct capabilities or limitations of intrusion detection systems.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS is able to identify and halt attacks while they are still in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported	0.25 LOW
2	An IDS can carry out forensic analysis after an attack has finished.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported	0.30 LOW
3	A passive detection system can only log and alert when an attack is identified.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 29 062 - Intrusion Detection System::s29::1	supported (stem gate)	0.67
4	A passive detection system is unable to actively stop an attack that is already underway.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 29 062 - Intrusion Detection System::s29::1	supported	0.33 LOW
5	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

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 2; 062 - Intrusion Detection System, slide 29

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

Explain the four classes of threats to computer systems and, for each class, identify the security service that counters it, as described in the introduction to computer security lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is a threat class involving unauthorized access to information, 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	0.40 LOW
2	Deception is a threat class involving acceptance of false data, countered by integrity services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.40 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Disruption is a threat class involving interruption or prevention of correct operation, countered by integrity services.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.46 LOW
4	Usurpation is a threat class involving unauthorized control of part of a system, 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	partly supported	0.46 LOW
5	A threat is only a potential violation of security, whereas an attack is 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)	0.50

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: 011 - Introduction to Computer Security, slide 10; 011 - Introduction to Computer Security, slide 9

PART B - QUESTION 2

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

Scenario:

A hospital is reviewing how its information systems decide whether a clinician may open a patient record. The review team wants to know what the access control subsystem is trying to achieve and which component is responsible for making each authorization decision before any record is released.

Question:

State five points about the goals of access control and the role of the reference monitor in authorization, as presented in the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Access control must determine, for a given subject, which objects it can access and in what manner.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.56
2	Access control must also determine, for a given object, which subjects can access it and in what manner.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.50
3	The 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	The goals of access control include granting, limiting, preventing and revoking access.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 4 023 - Access Control and Authorization::s04::1	supported (stem gate)	0.88
5	Reference monitors are the instruments used to realize access control policies and can be deployed at every level 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

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

Question:

The hospital review team is considering formal security models for controlling access to patient records. Explain five points about the Bell-La Padula, Biba and Chinese Wall models, covering the security concern each model addresses and the access rules that each model imposes.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula model is presented as a formal 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)	0.67
2	The Biba model is presented as a formal security model that adds integrity verification.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	0.57
3	The Chinese Wall model is presented as a formal 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)	0.62
4	The Chinese Wall simple security rule permits a subject to access an object only when the object lies within the same company dataset as previously accessed objects (inside the Wall) or in a completely different conflict of interest class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 25 024 - Formal Security Model::s25::1	supported	0.46 LOW
5	The Chinese Wall policy proposed by Brewer and Nash is strictly speaking 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)	0.54

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 25; 024 - Formal Security Model, slide 5

End of marking scheme.