



UNIVERSITI TEKNOLOGI MARA
MARKING SCHEME

COURSE	:	COMPUTER SECURITY
COURSE CODE	:	CSC662
EXAMINATION	:	OCTOBER 2026 (MOCK)
TIME	:	3 HOURS

MARKING SCHEME NOTES

1. This marking scheme accompanies the CSC662 mock paper (October 2026).
Computed answers show working; theory answers are supported by lecture slides (not lecturer-marked); verbatim quotes are omitted in this public build; slide citations are retained.
2. Supported theory marking points quote the lecture decks; any unresolved slot would remain a visible placeholder.
3. Part A = $10 \times (2 + 6)$; Part B = $2 \times (5 + 5)$; total = 100 marks.
4. Computed: 0 slot(s). Supported theory: 24 slots. Placeholders: 0.
Questions and answers are for local study use only.
5. Near-copy rejection used all 35 past papers; style widening is recorded per slot.

FOR MARKERS' USE ONLY

This marking scheme consists of 16 printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

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

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

Part A: 10 x (2 + 6) = 80 marks. Part B: 2 x (5 + 5) = 20 marks. Total: 100 marks. Slots: 0 computed, 24 supported by lecture slides, 0 placeholder.

Methods: computed answers use verified solvers. Theory answers are supported by lecture slides (not lecturer-marked). Each point carries a deck/slide citation and overlap score; verbatim quote text is omitted from this public build. Low overlap is flagged for human review.

PART A - QUESTION 1

A1a - 2 marks - supported by lecture slides (not lecturer-marked)

Question:

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Software insecurity arises because an attacker can alter system resources that are critical for program execution, such as the instruction pointer or function call addresses.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.67
2	A key source of software insecurity is the failure to validate user input.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 30 051 - Software Security::s30::1	supported (stem gate)	0.86

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

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

Citations: 051 - Software Security, slide 30

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

Question:

Windows provides a rich set of security mechanisms, yet its complexity is often described as its own worst enemy. Explain six aspects of Windows security mechanisms, covering their purpose, the components involved, and the risks that arise from their complexity.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Windows offers elaborate mechanisms for managing user accounts, objects and access control.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 21 041 - Windows Security::s21::1	supported (stem gate)	0.80
2	Discretionary access control 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 very complexity of these mechanisms means that 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 (stem gate)	0.50
4	Active Directory, introduced with Windows 2000, is an LDAP-like directory service used to organise system resources.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.91

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Active Directory manages users and groups, security credentials and certificates, and system resources such as desktops, servers and printers.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 6 041 - Windows Security::s06::1	supported (stem gate)	0.64
6	In Windows, subjects are processes and threads, and their security credentials are held in a token that is inherited 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)	0.58

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 2

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

Question:

Explain two characteristics of Trojan horse malware as described in the lecture, focusing on how it behaves and what harm it causes.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans disguise themselves as useful or benign programs so 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, a Trojan steals private data, deletes files, logs keystrokes or opens a way 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.

Citations: 051 - Software Security, slide 12

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

Question:

Explain six techniques or behaviours by which malware such as viruses, worms and rootkits propagate themselves or conceal their activity on an infected system, as described in the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can spread by infecting the boot sector of a disk, as illustrated by Elk Cloner spreading through boot sector infection.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.36 LOW
2	A worm can propagate across a network by exploiting a remote execution feature of a service, as the Morris worm did with sendmail.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.25 LOW
3	An executable COM virus appends its virus body to a program and redirects the program entry point to the virus code.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	partly supported	0.40 LOW
4	After running, the virus code restores the original entry point and jumps to it so the host program still appears to work.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.57
5	An EXE virus overwrites the program header so that the entry point switches to the virus.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 10 051 - Software Security::s10::1	supported (stem gate)	0.75

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	A rootkit hides malicious processes and software so that the attacker keeps privileged remote access, and it is hard to detect because it hides from the very tools used to find it.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	partly supported	0.44 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 7; 051 - Software Security, slide 9

PART A - QUESTION 3

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

Question:

Explain how a disclosure threat and a disruption threat each affect the confidentiality, integrity and availability of an information system, as described in the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A disclosure threat involves unauthorized access to information (through snooping, sniffing or wiretapping) and is countered by confidentiality services, so it harms confidentiality.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.29 LOW
2	A disruption threat interrupts or prevents correct operation of the system and is countered by integrity services, so it harms availability of correct operation.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.42 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

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

Question:

Discuss the Samy worm as a case study of a cross-site scripting attack, explaining how the malicious script was injected, how it spread between users, and what impact it had, as described in the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The attacker 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 user visiting an infected user's page had their own profile and friends list infected with the JavaScript.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.70
5	The worm ultimately infected about 1,000,000 MySpace profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.57

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

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

Citations: 052 - Web Security, slide 13; 052 - Web Security, slide 15

PART A - QUESTION 4

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

Question:

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

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A sensor can be positioned 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)	0.50
2	A sensor can be positioned on the DMZ.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 7 062 - Intrusion Detection System::s07::1	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: 062 - Intrusion Detection System, slide 7

A4b - 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 what each mechanism does to control or secure 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 acts as a firewall and web filter, provides shared network connections, and caches data to speed up common requests, improving data security and performance.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.83
3	Network segmentation creates 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 each user to only the access and permission 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	IDS/IPS detect or prevent network security 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)	0.86

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 5

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

Question:

List two formal security models named in the lecture and, for each, state the specific security concern it is designed to address.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula (BLP) model is identified as a formal security model concerned with access control.	[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 Chinese Wall model is identified as addressing conflicts of interest for 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)	0.88

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 27; 024 - Formal Security Model, slide 5

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

Question:

Discuss the access control structures used to implement access policies, covering the access control matrix, access control lists and capabilities, and explain the requirements such structures must satisfy.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Name the access control matrix as one of the structures for implementing access policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported (stem gate)	0.83
2	State that the access control matrix is a basic control structure whose advantages include 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	0.25 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	Identify the access control matrix's disadvantages as 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	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	Give one advantage of ACLs, such as easy access to an object's access rights or relative easiness of management using abstractions.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported	0.40 LOW
6	State the requirements that access control structures must meet, including expressing control policies, verifiability of correctness, and 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	0.23 LOW

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

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

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

PART A - QUESTION 6

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

Question:

Explain how the chain of trust is established in the Trusted Computing architecture, referring to the role of the TPM and the measurements taken during boot.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Each stage of the boot process measures and validates the next stage, with the resulting measurements recorded in the TPM's Platform Configuration Registers (PCRs).	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.31 LOW
2	The chain begins at the hardware TPM and then extends through software components such as the RTM, TPM Software Stack, BIOS and kernel.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 8 073 - Trusted Computing::s08::1	partly supported	0.39 LOW

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

Citations: 073 - Trusted Computing, slide 8

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

Question:

Describe the two primary system components of the Next Generation Secure Computing Base (NGSCB) and, for each component, state its role in the trusted platform.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is a special kernel that forms the core of the trusted operating environment.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 13 073 - Trusted Computing::s13::1	supported (stem gate)	0.62
2	Nexus is 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
3	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
4	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
5	The Nexus Computing Agent (NCA) is a trusted software component.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 15 073 - Trusted Computing::s15::1	supported	0.33 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 13; 073 - Trusted Computing, slide 14; 073 - Trusted Computing, slide 15

PART A - QUESTION 7

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

Question:

A biometric system performs identification and authentication through a sequence of stages. List TWO (2) stages that belong to the authentication stage of this process.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Comparison of the acquired biometric sample against the stored master characteristics	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 5 072 - Biometrics and Authentication::s05::1	partly supported	0.14 LOW
2	A decision reached on the outcome of the comparison	[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

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

State the definition of a biometric as given in the course, and state the two sectors into which today's biometric applications are categorised. Then state one example technology from each sector.

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	Such a characteristic can theoretically be used for identification or verification of identity.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 2 072 - Biometrics and Authentication::s02::1	supported (stem gate)	0.83
3	Biometric applications available today are categorised 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
4	The two sectors are the physiological (listed as 'psychological' in the slide) sector and the behavioural sector.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	partly supported	0.25 LOW
5	The second sector is the behavioural sector.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported	0.33 LOW
6	An example physiological technology is the fingerprint, which 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	partly supported	0.46 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 2; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 6

PART A - QUESTION 8**A8a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

Explain the difference between morals, ethics and laws as three forms of guidance for professional conduct in computer security.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief about right and wrong conduct, forming the bedrock 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)	0.82
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:

Refer to your answer in (a). Explain six requirements that a professional code of ethics and conduct, such as the ACM code, places on a computing professional working in computer security.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The professional must contribute to society and human well-being, recognising that all people are 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
2	The professional must avoid causing harm through 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
3	The professional must 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
4	The professional must honour confidentiality of information entrusted to them.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.14 LOW
5	The professional is expected to keep up high standards of competence, conduct and ethical practice in their 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)	0.70
6	The professional should only access computing and communication resources when authorised or when the public good compels 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)	0.75

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 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 user accounts to reduce the risk of password compromise.

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:**

State three motivations for adopting single sign-on, and state three design criteria that Kerberos satisfies as an SSO solution.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	One motivation for SSO is to reduce 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	One motivation for SSO is to reduce 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	One motivation for SSO is to reduce the effort of password maintenance.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.67
4	Kerberos provides security 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 provides reliability because every use of a service requires prior authentication.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 18 022 - Identification and Authentication::s18::1	supported (stem gate)	0.67

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Kerberos provides transparency because 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)	0.64

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

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

Citations: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18

PART A - QUESTION 10

A10a - 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, as described in the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can confirm 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	0.25 LOW
2	An 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

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

Question:

Compare the three security concepts of vulnerability, threat and attack as defined in the lecture, and explain how protection mechanisms are organised to counter threats to assets.

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 characterised 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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	A threat is also defined as an object, person or other entity representing 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)	0.82
5	An attack is defined as 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)	0.83
6	Protection of assets is organised around 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.

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

Citations: 011 - Introduction to Computer Security, slide 28; 011 - Introduction to Computer Security, slide 9

PART B - QUESTION 1

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

Question:

Explain the goals that access control pursues and the role of the reference monitor in authorization, then describe how reference monitors relate to access control policies and where they may be deployed in a system.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that access control has four goals: 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
2	Identify the reference monitor as 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
3	Explain that reference monitors are the instruments used to realize access control policies.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	1.00
4	Note that reference monitors 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)	0.56

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Explain that access control methods implement policies governing which subjects may access which objects and in what manner.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 18 023 - Access Control and Authorization::s18::1	supported (stem gate)	0.70

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

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

Question:

*State the Chinese Wall model's simple security rule and its *-property, explain the type of policy the model represents, and describe how its permissions behave over time.*

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The simple security rule permits a subject to access an object only when the object is either within the Wall (in the same company datasets as objects the subject has already accessed) 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 (stem gate)	0.52
2	The Chinese Wall *-property allows a write only if the simple security rule permits 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
3	The Chinese Wall policy is strictly speaking not an integrity policy but an access control confidentiality policy.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 21 024 - Formal Security Model::s21::1	supported (stem gate)	0.82
4	A subject may access information from any company provided it has never accessed information from a different company in the same conflict class.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.92
5	Permissions in the Chinese Wall model change dynamically, since the access 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.

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

PART B - QUESTION 2

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

Scenario:

A computing professional joins a group that has a documented set of acceptable behaviors, and the group defines which specific actions are appropriate or inappropriate. The group also publishes a code of ethics and professional conduct, but some members argue that such a code may not reflect the ethics of every member and is often not enforceable.

Question:

Explain five points about how a professional code of ethics, such as the ACM code, guides the ethical conduct of a computing professional, including what such a code is and the limitations of relying on it.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A code of ethics is a documented set of acceptable behaviors 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)	0.78
2	The code is defined 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	partly supported	0.25 LOW
3	The code identifies specific actions as either 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)	0.60
4	A limitation is that the code may not reflect the ethics of every member of the group.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported (stem gate)	0.78
5	Another limitation is that the code is often not enforceable because it is a code of conduct, not a legal document.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 9 071 - Ethics and Computer Security::s09::1	supported (stem gate)	0.60

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:**

Discuss five points on how privacy and organizational responsibility apply to the scenario, where the group publishes a code of ethics and professional conduct. Your answer should consider the ethical dimensions of handling personal information and the responsibilities the group and its members bear.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Privacy is an ethical concern in security that involves protecting an individual's personal information.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	partly supported	0.33 LOW
2	Organizations must ensure information accuracy, which concerns the authentication and fidelity of information held about people.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	partly supported	0.27 LOW
3	Responsibility extends to information property, namely who owns information about individuals and how it may be sold or exchanged.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported (stem gate)	0.64

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
4	Organizations must address information accessibility, that is, what information a person has the right to obtain about others and how it can be used.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 13 071 - Ethics and Computer Security::s13::1	supported (stem gate)	0.67
5	The group's published code of ethics and professional conduct, such as that of the ACM, is a formal organizational instrument for guiding members' responsible handling of privacy.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::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 13; 071 - Ethics and Computer Security, slide 7

End of marking scheme.