



UNIVERSITI TEKNOLOGI MARA
MARKING SCHEME

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

MARKING SCHEME NOTES

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

FOR MARKERS' USE ONLY

This marking scheme consists of 16 printed pages

CSC662 - MARKING SCHEME (MOCK OCTOBER 2026)

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

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

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

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

PART A - QUESTION 1

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

Question:

Explain two characteristics of Trojan horse malware, including how it presents itself to users and what it does once active on a host.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Trojans disguise themselves as useful or benign software so users install them willingly.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported	0.00 LOW
2	Once running, a Trojan steals private data, deletes files, records keystrokes, or opens a way for additional malware.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 12 051 - Software Security::s12::1	supported (stem gate)	0.57

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

Citations: 051 - Software Security, slide 12

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

Question:

State six techniques by which malware attacks and propagates, covering how virus code is attached to or substituted for a program's entry point, how early viruses spread through boot sectors, and how a worm used a mail service flaw to spread across a network.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A virus can be attached by appending the virus body onto an existing program file.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported	0.44 LOW
2	The virus saves the program's original entry point inside the virus body before taking control.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.55
3	The program's entry point is replaced with a jump into the virus body so the virus runs first.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.70
4	After running, the virus code restores the original entry point and then jumps to it so the host program still executes.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 9 051 - Software Security::s09::1	supported (stem gate)	0.64

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
5	Early malware such as Elk Cloner propagated by infecting the boot sector.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	partly supported	0.33 LOW
6	The Morris worm spread by exploiting a debugging feature of sendmail that allowed remote execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 7 051 - Software Security::s07::1	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 7; 051 - Software Security, slide 9

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 within 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:

Biometric technologies are increasingly deployed as an alternative to passwords. Explain the categories of biometric applications and the characteristics and drawbacks of the specific biometric technologies discussed in the course.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State the definition of a biometric as a physiological or behavioural characteristic that can distinguish one person from another and can 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)	0.90
2	Identify the two sectors into which biometric applications are categorised today.	[verbatim slide quote omitted in public build]	072 - Biometrics and Authentication, slide 4 072 - Biometrics and Authentication::s04::1	supported (stem gate)	0.83

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
3	List the physiological biometric technologies: 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
4	List the behavioural biometric technologies: 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	Explain that iris scanning reads the unique pattern of the iris, needs 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	Give the disadvantages of fingerprint biometrics, including racial issues, dirt and wounds, finger placement, large database processing and spoofing, so liveness checking 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 3

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

Question:

State TWO (2) key security models listed under formal security models in the lecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Bell-La Padula (BLP) model, described as an access control only model.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	1.00
2	The Chinese Wall model, described as identification of conflicts of interest.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 5 024 - Formal Security Model::s05::1	supported (stem gate)	1.00

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

Citations: 024 - Formal Security Model, slide 5

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

Question:

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

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Identify 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 capabilities are listed as a structure (C-List) alongside the ACM and ACL.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 7 023 - Access Control and Authorization::s07::1	supported	0.20 LOW
3	Explain that an ACL is an object-centred description of access rights.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.83
4	Give one advantage of ACLs: easy access to the access rights of an object.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported (stem gate)	0.67
5	Give one disadvantage of ACLs: difficulty of revocation.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 10 023 - Access Control and Authorization::s10::1	supported	0.25 LOW
6	State that the ACM is a basic control structure offering clarity of definition and easy verification.	[verbatim slide quote omitted in public build]	023 - Access Control and Authorization, slide 8 023 - Access Control and Authorization::s08::1	partly supported	0.44 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 4

A4a - 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 state what an attacker can achieve by exploiting 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 size of the destination buffer.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 23 051 - Software Security::s23::1	supported	0.23 LOW

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Because bounds are not checked, the excess data spills into adjacent higher stack memory, letting the attacker replace the return address and divert execution.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 21 051 - Software Security::s21::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: 051 - Software Security, slide 21; 051 - Software Security, slide 23

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

Question:

State six Windows security mechanisms or components, identifying for each what it does within the Windows security architecture.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The Security Reference Monitor in kernel mode performs ACL verification.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.50
2	The winlogon log-on process handles user logon in user mode.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	0.71
3	The Local Security Authority verifies and changes passwords and manages 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 holds 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 enforces limited user privileges.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 3 041 - Windows Security::s03::1	supported (stem gate)	1.00
6	Security credentials for a subject are kept in a token that maps principals to subjects and may carry extra security attributes.	[verbatim slide quote omitted in public build]	041 - Windows Security, slide 11 041 - Windows Security::s11::1	partly supported	0.36 LOW

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

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

Citations: 041 - Windows Security, slide 11; 041 - Windows Security, slide 3

PART A - QUESTION 5

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

Question:

Explain how spyware and adware differ in the harm they cause, identifying for each the security objective from the CIA triad that is affected.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Spyware harms confidentiality because it steals user logins and passwords and can compromise sensitive bank information.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	partly supported	0.31 LOW
2	Adware is largely harmless and merely annoying, generating popup ads that interrupt other programs rather than breaching a security objective.	[verbatim slide quote omitted in public build]	051 - Software Security, slide 13 051 - Software Security::s13::1	supported (stem gate)	0.56

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

Citations: 051 - Software Security, slide 13

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

Question:

Refer to your answer in (a). Based on the scenario in (a), justify how the Samy worm's use of cross-site scripting allowed it to spread automatically, giving six distinct points about its injection, propagation and impact.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	The worm injected JavaScript into a user profile by manipulating the document body.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.67
2	It retrieved the victim's list of friends by issuing a GET request to a user profile.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	partly supported	0.25 LOW
3	It added Samy as a friend by performing an XML-HTTP request on the addFriends page.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported (stem gate)	0.78
4	Any visitor to an infected profile had their own profile and friends list infected, enabling automatic onward spread.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.27 LOW
5	The worm's scale of impact was very large, eventually infecting about one million profiles.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 15 052 - Web Security::s15::1	supported	0.30 LOW
6	The underlying weakness was that the web application returned user input without filtering, making it a potential XSS vulnerability.	[verbatim slide quote omitted in public build]	052 - Web Security, slide 13 052 - Web Security::s13::1	supported (stem gate)	0.69

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 6

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

Question:

Explain the difference between morals, ethics and laws as three forms of guidance for conduct, giving the defining characteristic of each.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Morals are described as traditions of belief concerning right and wrong conduct, forming the basis of social behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.55
2	Ethics is characterised as a set of guiding beliefs, standards or ideals that permeates an individual or a community.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 5 071 - Ethics and Computer Security::s05::1	supported (stem gate)	0.70

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

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

Question:

Discuss how a professional code of ethics and conduct guides a computing professional's behaviour, referring to the ACM code and the professional bodies that maintain such codes. Support your discussion with six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	State that professional bodies such as the ACM publish a formal code of ethics and professional conduct for their members.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 7 071 - Ethics and Computer Security::s07::1	supported (stem gate)	0.50
2	Explain that ethics is a documented set of acceptable behaviours defined by 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)	0.67
3	Note that the code identifies which specific actions are appropriate or inappropriate for the professional.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 6 071 - Ethics and Computer Security::s06::1	supported (stem gate)	0.50
4	Describe the expectation that the professional avoids harm and remains honest and trustworthy in their work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported (stem gate)	0.50
5	Describe the expectation that the professional respects privacy and honours confidentiality of information.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 11 071 - Ethics and Computer Security::s11::1	supported	0.43 LOW
6	Explain that the professional must 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

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 7

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

Question:

State TWO (2) facts about the chain of trust in the Trusted Computing architecture, including how measurements are recorded and where the chain begins.

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

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

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

Citations: 073 - Trusted Computing, slide 8

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

Question:

Describe the two primary system components of the Next Generation Secure Computing Base (NGSCB), explaining the role of each component and how they relate to one another.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Nexus is 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 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 and provides the application interface to the TPM.	[verbatim slide quote omitted in public build]	073 - Trusted Computing, slide 14 073 - Trusted Computing::s14::1	partly supported	0.38 LOW
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 (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 8

A8a - 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 architecture.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
2	Sensors are placed 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.

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

Citations: 062 - Intrusion Detection System, slide 7

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

Question:

Compare the preventive roles of a firewall and a remote access VPN in network security, and explain how an intrusion detection system complements these preventive mechanisms. Provide six distinct points.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	A firewall is a preventive mechanism that controls incoming and outgoing network traffic according to predefined security policies.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.58
2	A remote access VPN is a preventive mechanism that 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)	0.73
3	An IDS monitors network resources to detect intrusions and attacks that preventive techniques such as firewalls and proxy servers failed to stop.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 3 062 - Intrusion Detection System::s03::1	supported (stem gate)	0.80
4	A proxy server acts as a firewall and web filter, so it is another preventive mechanism that improves data security and network performance.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.57
5	Network segmentation creates boundaries between network segments whose assets share a common function, risk or role, thereby limiting exposure.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 3 061 - Network Security::s03::1	supported (stem gate)	0.60
6	IDS/IPS detect or prevent 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)	0.85

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

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

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

PART A - QUESTION 9

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

Question:

List TWO (2) advantages of having an organizational ethical code that clarify how technology professionals should behave.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	It makes acceptable standards of behaviour clearer to understand.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 8 071 - Ethics and Computer Security::s08::1	supported (stem gate)	0.50
2	It spreads shared guidelines that everyone is 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 (stem gate)	0.50

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

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

Citations: 071 - Ethics and Computer Security, slide 8

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

Question:

Describe six responsibilities that information specialists and general users carry when handling data within ethical, moral and legal constraints, and explain why merely describing these moral and ethical dimensions of ICT is not sufficient for organizational privacy protection.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Information specialists specifically are expected to act within ethical, moral and legal limits when doing their work.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.50
2	Ordinary users, not only specialists, also bear definite responsibilities for staying within ethical, moral and legal constraints.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported	0.27 LOW
3	Simply describing the moral and ethical dimensions of ICT is not enough; organizations must go beyond description.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	supported (stem gate)	0.64
4	Organizations must actively discuss the moral and ethical dimensions of ICT rather than only describing them.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 3 071 - Ethics and Computer Security::s03::1	partly supported	0.36 LOW
5	A person who is separated from law and justice is described as the worst of all animals, showing the need for legal and just conduct.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 4 071 - Ethics and Computer Security::s04::1	supported	0.39 LOW
6	A perfected person is the best of animals, implying that ethical development supports responsible behaviour.	[verbatim slide quote omitted in public build]	071 - Ethics and Computer Security, slide 4 071 - Ethics and Computer Security::s04::1	supported	0.30 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 10**A10a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

List TWO (2) password security controls that can be applied to protect password files and user accounts.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Apply access control to 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	0.44 LOW
2	De-activate user accounts after multiple 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)	0.75

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

Citations: 022 - Identification and Authentication, slide 12

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

Explain how single sign-on reduces the burden of authentication for users, and describe how Kerberos and smart cards support authentication in distributed environments.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Single sign-on reduces the need for users to memorize multiple passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.50
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 lowers the effort needed to maintain passwords.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported	0.29 LOW
4	Kerberos is a client-server architecture used to achieve single sign-on.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 16 022 - Identification and Authentication::s16::1	supported (stem gate)	0.57
5	In Kerberos login, the hash of the user's password becomes the user's secret key.	[verbatim slide quote omitted in public build]	022 - Identification and Authentication, slide 19 022 - Identification and Authentication::s19::1	supported (stem gate)	0.71

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
6	Smart cards are an alternative authentication mechanism 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)	0.62

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

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

PART B - QUESTION 1

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

Question:

Discuss five ways in which intrusion detection and related defensive mechanisms can help detect and defend against malware attacks on the company's systems.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	An IDS can detect malicious activity occurring in computer systems.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported (stem gate)	0.62
2	An IDS can identify and stop attacks that are currently in progress.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 2 062 - Intrusion Detection System::s02::1	supported (stem gate)	0.50
3	A passive detection system can 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)	0.75
4	Misuse detection systems can recognise known bad behaviour by matching attack patterns or signatures.	[verbatim slide quote omitted in public build]	062 - Intrusion Detection System, slide 17 062 - Intrusion Detection System::s17::1	partly supported	0.17 LOW
5	Sandboxing provides a safe, isolated environment in which to run or open suspected insecure programs or files.	[verbatim slide quote omitted in public build]	061 - Network Security, slide 26 061 - Network Security::s26::1	supported (stem gate)	0.82

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

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

Citations: 061 - Network Security, slide 26; 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 five classes of threats to information systems and, for each class, identify the security service that counters it.

Marking points:

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

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	Disclosure is a threat class involving unauthorized access to information, and confidentiality services are the countermeasure.	[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 in which false data is accepted, and integrity services counter this threat.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	partly supported	0.44 LOW
3	Disruption is a threat class that interrupts or prevents correct operation, and integrity services counter it.	[verbatim slide quote omitted in public build]	011 - Introduction to Computer Security, slide 10 011 - Introduction to Computer Security::s10::1	supported (stem gate)	0.50
4	Usurpation is a threat class involving unauthorized control of part of a system, and availability services counter it.	[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 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)	0.57

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

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

Citations: 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)

Question:

State the four goals of access control and explain the role of a reference monitor in authorization. Then describe how the Chinese Wall policy constrains a consultant's access to company information, and explain why this policy is described as history-sensitive.

Marking points:

No.	Point (1 mark)	Evidence quote	Source	Verdict	Overlap
1	List the four access control 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)	1.00
2	State that 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
3	Explain that reference monitors realize access control policies and can be placed 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)	0.83
4	Describe the simple Chinese Wall rule: a subject may read a company's information only if it has not already accessed information from another 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)	0.50
5	Explain that permissions under the Chinese Wall change dynamically because the rights a subject holds depend on its history of past accesses.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 24 024 - Formal Security Model::s24::1	supported (stem gate)	0.64

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

Citations: 023 - Access Control and Authorization, slide 18; 023 - Access Control and Authorization, slide 4; 024 - Formal Security Model, slide 24

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

Question:

Explain the Chinese Wall policy as a formal security model, covering the two rules that govern read and write access, the type of policy it is classified as, and the specific problem it was designed to solve.

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 in the same company dataset as objects the subject has already accessed (i.e., within 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 (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)	0.73
3	Strictly speaking the Chinese Wall is 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	The policy was designed by Brewer and Nash to address a very specific concern, namely conflicts of interest faced by a consultant or contractor.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported (stem gate)	0.92
5	The model illustrates that security policies can be crafted to solve very specialized problems.	[verbatim slide quote omitted in public build]	024 - Formal Security Model, slide 27 024 - Formal Security Model::s27::1	supported (stem gate)	0.60

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

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

slide 26; 024 - Formal Security Model, slide 27

End of marking scheme.