



---

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 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 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 formal security models used for access control, stating the specific security concern each model is designed to address.*

##### Marking points:

| No. | Point (1 mark)                                                                                                                                         | Evidence quote                                 | Source                                                                       | Verdict               | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | The Chinese Wall model is a confidentiality access control policy that addresses conflicts of interest for consultants or contractors.                 | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 21<br>024 - Formal Security Model::s21::1 | partly supported      | 0.33<br>LOW |
| 2   | The Chinese Wall policy is crafted to solve the specialized problem of conflicts of interest, showing that policies can target very specific concerns. | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 27<br>024 - Formal Security Model::s27::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: 024 - Formal Security Model, slide 21; 024 - Formal Security Model, slide 27*

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

##### Question:

*State six points about the access control matrix, access control lists and capability lists as access control structures, covering what each structure represents and one advantage or disadvantage of each.*

##### Marking points:

| No. | Point (1 mark)                                                                                        | Evidence quote                                 | Source                                                                                            | Verdict   | Overlap     |
|-----|-------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------|-------------|
| 1   | The access control matrix is described as a basic control structure for implementing access policies. | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 8<br>023 - Access Control and Authorization::s08::1 | supported | 0.43<br>LOW |
| 2   | A strength of the access control matrix is that it is clearly defined and easy to verify.             | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 8<br>023 - Access Control and Authorization::s08::1 | supported | 0.25<br>LOW |

| No. | Point (1 mark)                                                                               | Evidence quote                                 | Source                                                                                             | Verdict               | Overlap     |
|-----|----------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------------------|-----------------------|-------------|
| 3   | A weakness of the access control matrix is that it scales poorly and handles changes poorly. | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 8<br>023 - Access Control and Authorization::s08::1  | supported             | 0.38<br>LOW |
| 4   | An access control list is an object-centred description of access rights.                    | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 10<br>023 - Access Control and Authorization::s10::1 | supported (stem gate) | 0.67        |
| 5   | A capability list is a subject-centred description of access rights.                         | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 9<br>023 - Access Control and Authorization::s09::1  | supported (stem gate) | 0.67        |
| 6   | A disadvantage of capability lists is that they require extra integrity protection.          | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 9<br>023 - Access Control and Authorization::s09::1  | supported             | 0.43<br>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 8; 023 - Access Control and Authorization, slide 9*

## PART A - QUESTION 2

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

#### Question:

*Explain how NIDS sensors should be positioned in a network, giving the typical sensor locations.*

#### Marking points:

| No. | Point (1 mark)                                                                                                                                             | Evidence quote                                 | Source                                                                                | Verdict               | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Sensors must be placed strategically so that the most valuable assets are defended.                                                                        | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 7<br>062 - Intrusion Detection System::s07::1 | supported (stem gate) | 0.88        |
| 2   | Typical sensor locations include just inside the firewall, on the DMZ, on the server farm segment, and on segments connecting mainframe or midrange hosts. | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 7<br>062 - Intrusion Detection System::s07::1 | partly supported      | 0.20<br>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*

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

#### Question:

*Describe six preventive network security mechanisms that an organization can deploy to protect its network, explaining the role each mechanism plays.*

**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<br>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<br>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<br>061 - Network Security::s03::1 | supported (stem gate) | 0.77    |
| 4   | A remote access VPN gives individual hosts or clients secure access to the organization network from remote locations.                      | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 4<br>061 - Network Security::s04::1 | supported (stem gate) | 0.80    |
| 5   | Zero Trust Network Access limits each user to only the access and permissions needed to fulfil their role.                                  | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 4<br>061 - Network Security::s04::1 | supported (stem gate) | 0.55    |
| 6   | IDS/IPS mechanisms detect or prevent network attacks such as brute force, denial-of-service and exploitation of network vulnerabilities.    | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 4<br>061 - Network Security::s04::1 | supported (stem gate) | 0.79    |

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

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

## PART A - QUESTION 3

### A3a - 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<br>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<br>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*

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

**Question:**

*Explain the roles of the two primary system components of the Next Generation Secure Computing Base (NGSCB), describing what each component is and how it supports trusted operation of the platform.*

**Marking points:**

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

| No. | Point (1 mark)                                                                                                   | Evidence quote                                 | Source                                                               | Verdict               | Overlap |
|-----|------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|---------|
| 1   | Nexus is described as a special kernel that forms the core of the trusted operating environment.                 | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 13<br>073 - Trusted Computing::s13::1 | supported (stem gate) | 0.62    |
| 2   | Nexus acts as a security kernel that is authenticated on boot.                                                   | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 14<br>073 - Trusted Computing::s14::1 | supported (stem gate) | 0.67    |
| 3   | Nexus authenticates trusted programs.                                                                            | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 14<br>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<br>073 - Trusted Computing::s14::1 | supported (stem gate) | 0.60    |
| 5   | Nexus does not trust the operating system.                                                                       | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 14<br>073 - Trusted Computing::s14::1 | supported (stem gate) | 0.50    |
| 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<br>073 - Trusted Computing::s15::1 | supported (stem gate) | 0.62    |

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

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

## PART A - QUESTION 4

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

#### Question:

*State TWO (2) differences between morals and laws as described in the lecture on ethics and computer security.*

#### Marking points:

| No. | Point (1 mark)                                                                                                      | Evidence quote                                 | Source                                                                                    | Verdict               | Overlap |
|-----|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------|---------|
| 1   | Morals are described as traditions of belief concerning right and wrong conduct within a society.                   | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 5<br>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<br>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*

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

#### Question:

*State SIX (6) professional conduct requirements that the ACM code expects a computing professional to follow when carrying out computing work.*

**Marking points:**

| No. | Point (1 mark)                                                                                                   | Evidence quote                                 | Source                                                                                     | Verdict               | Overlap |
|-----|------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------|---------|
| 1   | The professional must aim for high quality in the processes and products of their professional work.             | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 12<br>071 - Ethics and Computer Security::s12::1 | supported (stem gate) | 0.75    |
| 2   | The professional must keep up high standards of competence, conduct and ethical practice.                        | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 12<br>071 - Ethics and Computer Security::s12::1 | supported (stem gate) | 0.78    |
| 3   | The professional must be aware of and respect the existing rules that apply to professional work.                | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 12<br>071 - Ethics and Computer Security::s12::1 | supported (stem gate) | 0.62    |
| 4   | The professional must give thorough evaluations of computer systems and their impacts, including possible risks. | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 12<br>071 - Ethics and Computer Security::s12::1 | supported (stem gate) | 0.80    |
| 5   | The professional must only perform work that falls within their areas of competence.                             | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 12<br>071 - Ethics and Computer Security::s12::1 | supported (stem gate) | 0.56    |
| 6   | The professional must design and implement systems that are secure in a robust and usable way.                   | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 12<br>071 - Ethics and Computer Security::s12::1 | supported (stem gate) | 0.67    |

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

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

*Citations: 071 - Ethics and Computer Security, slide 12*

**PART A - QUESTION 5****A5a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

*Explain two characteristics of Trojan horse malware that distinguish its behaviour on an infected host.*

**Marking points:**

| No. | Point (1 mark)                                                                                                          | Evidence quote                                 | Source                                                               | Verdict               | Overlap     |
|-----|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|-------------|
| 1   | Trojans disguise themselves as legitimate or benign software so users install them willingly.                           | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 12<br>051 - Software Security::s12::1 | supported             | 0.00<br>LOW |
| 2   | Once running, a trojan steals private data, deletes files, records keystrokes, or opens a backdoor for further malware. | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 12<br>051 - Software Security::s12::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: 051 - Software Security, slide 12*

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

*Discuss six malware attack techniques and propagation methods, explaining how each technique operates and the impact it has on an infected system or its users.*

**Marking points:**

| No. | Point (1 mark)                                                                                                                                            | Evidence quote                                 | Source                                                               | Verdict               | Overlap     |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|-------------|
| 1   | Rootkits conceal malicious processes and software on the infected system so that the attacker retains privileged remote access.                           | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 13<br>051 - Software Security::s13::1 | supported (stem gate) | 0.75        |
| 2   | Rootkits are typically installed after a vulnerability has been discovered, allowing the infected machine to remain under the malware author's control.   | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 13<br>051 - Software Security::s13::1 | supported (stem gate) | 0.60        |
| 3   | Spyware steals user credentials and records activity such as visited sites and keystrokes, which can lead to identity theft and compromised bank details. | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 13<br>051 - Software Security::s13::1 | partly supported      | 0.29<br>LOW |
| 4   | A virus can be attached to an executable by appending the virus body to the host program.                                                                 | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 10<br>051 - Software Security::s10::1 | supported (stem gate) | 0.50        |
| 5   | A virus can hijack execution by overwriting the program header so that the entry point switches to the virus code.                                        | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 10<br>051 - Software Security::s10::1 | supported (stem gate) | 0.55        |
| 6   | The Morris worm propagated across the Arpanet by exploiting a debugging feature of sendmail that permitted remote execution.                              | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 7<br>051 - Software Security::s07::1  | partly supported      | 0.36<br>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: 051 - Software Security, slide 10; 051 - Software Security, slide 13; 051 - Software Security, slide 7*

## PART A - QUESTION 6

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

**Question:**

*State the four goals of access control and identify the component that makes authorization decisions.*

**Marking points:**

| No. | Point (1 mark)                                                                                           | Evidence quote                                 | Source                                                                                            | Verdict               | Overlap |
|-----|----------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------|---------|
| 1   | The goals of access control are granting access, limiting access, preventing access and revoking access. | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 4<br>023 - Access Control and Authorization::s04::1 | supported (stem gate) | 1.00    |
| 2   | Authorization decisions are made by the reference monitor.                                               | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 4<br>023 - Access Control and Authorization::s04::1 | supported (stem gate) | 0.80    |

*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 4*

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

**Question:**

Refer to your answer in (a). Explain six points about the formal security models used for access control, covering the Bell-La Padula model, the Biba model and the Chinese Wall model, including the security concern each addresses and the rules that govern access under the Chinese Wall model.

**Marking points:**

| No. | Point (1 mark)                                                                                                                                                                                                                                       | Evidence quote                                 | Source                                                                       | Verdict               | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | The Bell-La Padula model is a formal security model that deals with access control only.                                                                                                                                                             | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 5<br>024 - Formal Security Model::s05::1  | supported (stem gate) | 0.67        |
| 2   | The Biba model is a formal security model that adds integrity verification.                                                                                                                                                                          | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 5<br>024 - Formal Security Model::s05::1  | supported (stem gate) | 0.57        |
| 3   | The Chinese Wall model is concerned with identifying conflicts of interest.                                                                                                                                                                          | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 5<br>024 - Formal Security Model::s05::1  | supported (stem gate) | 0.83        |
| 4   | The Chinese Wall simple security rule permits a subject to access an object only when that object lies within the subject's existing Wall (the same company datasets already accessed) or falls in a completely separate conflict of interest class. | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 25<br>024 - Formal Security Model::s25::1 | supported             | 0.46<br>LOW |
| 5   | Under the Chinese Wall *-property, a write is allowed only when the simple security rule permits it and the subject cannot read any unsanitized object belonging to a different company dataset from the one being written to.                       | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 26<br>024 - Formal Security Model::s26::1 | supported             | 0.46<br>LOW |
| 6   | In the Chinese Wall policy, permissions change dynamically because a subject's access rights depend on the history of past accesses.                                                                                                                 | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 24<br>024 - Formal Security Model::s24::1 | supported (stem gate) | 0.69        |

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 25; 024 - Formal Security Model, slide 26; 024 - Formal Security Model, slide 5

**PART A - QUESTION 7****A7a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

List TWO (2) key points about software insecurity and buffer overflows as presented in the Software Security lecture.

**Marking points:**

| No. | Point (1 mark)                                                                                                                                                                  | Evidence quote                                 | Source                                                               | Verdict               | Overlap |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|---------|
| 1   | Software insecurity arises because an attacker can modify 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<br>051 - Software Security::s30::1 | supported (stem gate) | 0.72    |

| No. | Point (1 mark)                                                                        | Evidence quote                                 | Source                                                               | Verdict               | Overlap |
|-----|---------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|---------|
| 2   | A major source of software insecurity is the failure to properly validate user input. | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 30<br>051 - Software Security::s30::1 | supported (stem gate) | 0.67    |

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

*Citations: 051 - Software Security, slide 30*

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

#### Question:

*Compare the security mechanisms found in Windows with those found in UNIX, focusing on the strengths and weaknesses of each. Provide six (6) distinct points covering user account and object management, access control, administration requirements, and missing features.*

#### Marking points:

| No. | Point (1 mark)                                                                                                                                                                       | Evidence quote                                 | Source                                                             | Verdict               | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------|-----------------------|-------------|
| 1   | Windows provides complex built-in mechanisms for managing user accounts and objects as well as controlling access.                                                                   | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 21<br>041 - Windows Security::s21::1 | supported (stem gate) | 0.83        |
| 2   | The very complexity of Windows security can backfire, since misconfiguration or implementation bugs can cause serious security incidents.                                            | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 21<br>041 - Windows Security::s21::1 | supported             | 0.46<br>LOW |
| 3   | UNIX offers a set of flexible security mechanisms, but their effectiveness depends on careful and knowledgeable administration.                                                      | [verbatim slide quote omitted in public build] | 042 - Linux Security, slide 28<br>042 - Linux Security::s28::1     | supported (stem gate) | 0.58        |
| 4   | UNIX lacks several key features suggested by security models, such as ACLs or security levels.                                                                                       | [verbatim slide quote omitted in public build] | 042 - Linux Security, slide 28<br>042 - Linux Security::s28::1     | supported (stem gate) | 0.78        |
| 5   | The main security strength of UNIX comes from its open source implementation, which allows flaws to be discovered and fixed early.                                                   | [verbatim slide quote omitted in public build] | 042 - Linux Security, slide 28<br>042 - Linux Security::s28::1     | supported (stem gate) | 0.58        |
| 6   | Windows security mechanisms include discretionary access control (DACS) that enable fine-grained access control of heterogeneous entities in Windows itself as well as applications. | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 21<br>041 - Windows Security::s21::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: 041 - Windows Security, slide 21; 042 - Linux Security, slide 28*

## PART A - QUESTION 8

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

#### Question:

*List two classes of threats and, for each, state which security objective (confidentiality, integrity or availability) is affected and which service counters it.*

#### Marking points:

| No. | Point (1 mark)                                                                                                      | Evidence quote                                 | Source                                                                                               | Verdict          | Overlap     |
|-----|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------|-------------|
| 1   | Disclosure is a threat class involving unauthorized access to information, and confidentiality services counter it. | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 10<br>011 - Introduction to Computer Security::s10::1 | partly supported | 0.40<br>LOW |

| No. | Point (1 mark)                                                                                     | Evidence quote                                 | Source                                                                                               | Verdict          | Overlap     |
|-----|----------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------|-------------|
| 2   | Deception is a threat class involving acceptance of false data, and integrity services counter it. | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 10<br>011 - Introduction to Computer Security::s10::1 | partly supported | 0.40<br>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: 011 - Introduction to Computer Security, slide 10*

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

#### Question:

*The Samy worm spread through MySpace by exploiting a cross-site scripting flaw. Explain six aspects of this incident, covering how the JavaScript was injected, how the worm propagated through user profiles and friend lists, 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 by writing to document.body.innerHTML.                                                                                                  | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 15<br>052 - Web Security::s15::1 | supported (stem gate) | 0.70        |
| 2   | The worm obtained the list of a user's heroes by issuing a GET request on a user profile.                                                                                                | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 15<br>052 - Web Security::s15::1 | supported             | 0.38<br>LOW |
| 3   | The worm 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<br>052 - Web Security::s15::1 | supported (stem gate) | 0.70        |
| 4   | Any visitor to an infected user's page had their own profile and friends list infected with the JavaScript and with Samy.                                                                | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 15<br>052 - Web Security::s15::1 | supported (stem gate) | 0.64        |
| 5   | The infection ultimately reached approximately 1,000,000 MySpace profiles.                                                                                                               | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 15<br>052 - Web Security::s15::1 | supported             | 0.43<br>LOW |
| 6   | The underlying flaw is that any web application returning user input without filtering is a potential XSS vulnerability, permitting arbitrary JavaScript to run in the victim's browser. | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 13<br>052 - Web Security::s13::1 | supported (stem gate) | 0.53        |

*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 9

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

#### Question:

*Explain the two stages of the biometric authentication process and state what happens during 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<br>072 - Biometrics and Authentication::s05::1 | supported | 0.33<br>LOW |

| No. | Point (1 mark)                                                                                                | Evidence quote                                 | Source                                                                                      | Verdict               | Overlap |
|-----|---------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------|---------|
| 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<br>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*

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

#### Question:

*A bank plans to deploy biometric authentication at its branch counters. Explain the biometric mechanisms and technologies involved, covering how biometrics are defined, the categories of biometric applications, and the characteristics and drawbacks of specific technologies.*

#### 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 and can theoretically be used for identification or verification of identity. | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 2<br>072 - Biometrics and Authentication::s02::1  | supported (stem gate) | 0.92        |
| 2   | Biometric applications are categorized into two sectors: physiological and behavioural.                                                                                                                             | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 4<br>072 - Biometrics and Authentication::s04::1  | supported (stem gate) | 0.71        |
| 3   | Physiological biometrics include iris, fingerprints, hand, retinal and face recognition.                                                                                                                            | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 4<br>072 - Biometrics and Authentication::s04::1  | supported (stem gate) | 0.67        |
| 4   | Behavioural biometrics include voice, typing pattern and signature.                                                                                                                                                 | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 4<br>072 - Biometrics and Authentication::s04::1  | supported (stem gate) | 0.67        |
| 5   | Iris scanning reads the unique pattern of the iris, requires no touch, and overcomes issues of retinal scanners.                                                                                                    | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 10<br>072 - Biometrics and Authentication::s10::1 | partly supported      | 0.36<br>LOW |
| 6   | Fingerprint biometrics suffer disadvantages such as racial issues, dirt, grime and wounds, finger placement, large database processing, and spoofing so liveness is important.                                      | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 7<br>072 - Biometrics and Authentication::s07::1  | partly supported      | 0.17<br>LOW |

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

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

**PART A - QUESTION 10****A10a - 2 marks - supported by lecture slides (not lecturer-marked)****Question:**

*Explain two password security controls that a system administrator can apply to protect password files and accounts.*

**Marking points:**

| No. | Point (1 mark)                                                        | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap |
|-----|-----------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|---------|
| 1   | Access control should be applied to the password files themselves.    | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 12<br>022 - Identification and Authentication::s12::1 | supported (stem gate) | 0.57    |
| 2   | Accounts should be de-activated after multiple failed login attempts. | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 12<br>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:**

*Describe six aspects of single sign-on and Kerberos as authentication mechanisms in large distributed environments, covering the motivation for single sign-on, the solutions available, the design criteria of Kerberos, and how a user logs in to Kerberos.*

**Marking points:**

| No. | Point (1 mark)                                                                                         | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Single sign-on reduces the need for users to memorize passwords.                                       | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 16<br>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<br>022 - Identification and Authentication::s16::1 | supported             | 0.43<br>LOW |
| 3   | Single sign-on reduces the effort of password maintenance.                                             | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 16<br>022 - Identification and Authentication::s16::1 | supported (stem gate) | 0.67        |
| 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<br>022 - Identification and Authentication::s18::1 | supported (stem gate) | 0.60        |

| No. | Point (1 mark)                                                                                                                                         | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|---------|
| 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<br>022 - Identification and Authentication::s18::1 | supported (stem gate) | 0.70    |
| 6   | During Kerberos login, the user enters a user name and password at a client workstation, and the hash of the password becomes the client's secret key. | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 19<br>022 - Identification and Authentication::s19::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 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:

*An organisation deploys an intrusion detection system to defend its network against malware and other attacks. Explain five aspects of how such detection and defence mechanisms work, covering what the IDS does, how misuse detection recognises attacks, and the limitations of these approaches.*

#### Marking points:

| No. | Point (1 mark)                                                                                                                  | Evidence quote                                 | Source                                                                                 | Verdict               | Overlap     |
|-----|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | The IDS detects malicious activity occurring in computer systems.                                                               | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 2<br>062 - Intrusion Detection System::s02::1  | supported (stem gate) | 0.71        |
| 2   | The IDS can identify and stop attacks that are currently in progress.                                                           | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 2<br>062 - Intrusion Detection System::s02::1  | supported (stem gate) | 0.50        |
| 3   | Misuse detection represents attacks as patterns or signatures so that even variations of the same attack can be detected.       | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 17<br>062 - Intrusion Detection System::s17::1 | supported (stem gate) | 0.90        |
| 4   | Misuse detection is of little use against unknown attack methods, since it only recognises known bad behaviour.                 | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 17<br>062 - Intrusion Detection System::s17::1 | supported             | 0.46<br>LOW |
| 5   | A passive detection system can only log and alert when an attack is identified, and cannot actively stop an attack in progress. | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 29<br>062 - Intrusion Detection System::s29::1 | supported             | 0.39<br>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 17; 062 - Intrusion Detection System, slide 2; 062 - Intrusion Detection System, slide 29*

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

*State five distinct threat classes or attack techniques that can compromise a computer system, and for each one identify a countermeasure or defence mechanism that addresses it.*

**Marking points:**

| No. | Point (1 mark)                                                                                                                           | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Threats are potential violations of security, distinct from attacks which are actual violations.                                         | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 9<br>011 - Introduction to Computer Security::s09::1  | supported (stem gate) | 0.67        |
| 2   | Forces of nature are dangerous threats that disrupt information storage, transmission and use, requiring controls and contingency plans. | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 13<br>011 - Introduction to Computer Security::s13::1 | partly supported      | 0.33<br>LOW |
| 3   | Software threats include modification of program code and viruses/self-replicating code.                                                 | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 2<br>051 - Software Security::s02::1                                  | partly supported      | 0.22<br>LOW |
| 4   | Code injection attacks such as XSS and SQL injection are software threats that must be defended against.                                 | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 2<br>051 - Software Security::s02::1                                  | partly supported      | 0.18<br>LOW |
| 5   | Input cleansing and validation is a defence mechanism that models expected input and discards what does not fit.                         | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 29<br>051 - Software Security::s29::1                                 | partly supported      | 0.27<br>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: 011 - Introduction to Computer Security, slide 13; 011 - Introduction to Computer Security, slide 9; 051 - Software Security, slide 2; 051 - Software Security, slide 29*

**PART B - QUESTION 2****B2a - 5 marks - supported by lecture slides (not lecturer-marked)****Question:**

*Explain five ethical obligations that the ACM code expects a computing professional to uphold when developing and deploying technology, and explain why such a professional code may not always be enforceable.*

**Marking points:**

| No. | Point (1 mark)                                                                                                                         | Evidence quote                                 | Source                                                                                     | Verdict   | Overlap     |
|-----|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------|-----------|-------------|
| 1   | The professional should work for the benefit of society and human welfare, recognising that everyone affected counts as a stakeholder. | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 11<br>071 - Ethics and Computer Security::s11::1 | supported | 0.25<br>LOW |
| 2   | The professional should refrain from causing harm through computing work.                                                              | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 11<br>071 - Ethics and Computer Security::s11::1 | supported | 0.12<br>LOW |
| 3   | The professional should act truthfully and in a manner that earns trust.                                                               | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 11<br>071 - Ethics and Computer Security::s11::1 | supported | 0.00<br>LOW |

| No. | Point (1 mark)                                                                                             | Evidence quote                                 | Source                                                                                     | Verdict   | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------|-----------|-------------|
| 4   | The professional should safeguard personal data and the private information of others.                     | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 11<br>071 - Ethics and Computer Security::s11::1 | supported | 0.00<br>LOW |
| 5   | The code may fail to be enforceable because it functions as a conduct code rather than a legal instrument. | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 9<br>071 - Ethics and Computer Security::s09::1  | supported | 0.27<br>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 11; 071 - Ethics and Computer Security, slide 9*

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

### **Question:**

*Discuss the ethical concerns raised by the staff member's action and the company's responsibility, referring to privacy, the ACM code of ethics, and the nature of professional ethical codes.*

### **Marking points:**

| No. | Point (1 mark)                                                                                                                                                          | Evidence quote                                 | Source                                                                                     | Verdict               | Overlap     |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Explain that privacy concerns protecting an individual's personal information, which the staff member failed to do.                                                     | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 13<br>071 - Ethics and Computer Security::s13::1 | partly supported      | 0.33<br>LOW |
| 2   | Explain that information accessibility concerns what information a person has the right to obtain about others and how it can be used, which the staff member violated. | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 13<br>071 - Ethics and Computer Security::s13::1 | supported (stem gate) | 0.61        |
| 3   | State that the ACM has a code of ethics and professional conduct that the staff member should have followed.                                                            | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 7<br>071 - Ethics and Computer Security::s07::1  | supported (stem gate) | 0.55        |
| 4   | Describe ethics as a documented set of acceptable behaviors for professional groups that identifies specific actions as appropriate or inappropriate.                   | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 6<br>071 - Ethics and Computer Security::s06::1  | supported (stem gate) | 0.60        |
| 5   | Explain that because ethics are defined by the group, the company must enforce its own acceptable behavior standards rather than relying on external law.               | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 6<br>071 - Ethics and Computer Security::s06::1  | partly supported      | 0.12<br>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 6; 071 - Ethics and Computer Security, slide 7*

*End of marking scheme.*