



---

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: 1 slot(s). Supported theory: 23 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: 1 computed, 23 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:

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

##### Marking points:

| No. | Point (1 mark)                                      | Evidence quote                                 | Source                                                                                | Verdict               | Overlap     |
|-----|-----------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Sensors can be positioned just inside the firewall. | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 7<br>062 - Intrusion Detection System::s07::1 | supported (stem gate) | 0.50        |
| 2   | Sensors can be positioned on the DMZ.               | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 7<br>062 - Intrusion Detection System::s07::1 | supported             | 0.25<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*

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

##### Question:

*Explain three preventive network security mechanisms that an organization can deploy to protect its network, and for each mechanism describe how it controls or secures network traffic.*

##### Marking points:

| No. | Point (1 mark)                                                                                                                                       | Evidence quote                                 | Source                                                            | Verdict               | Overlap |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------|-----------------------|---------|
| 1   | A firewall controls incoming and outgoing network traffic according to predetermined security policies.                                              | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 3<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 network 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 network 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    |

| No. | Point (1 mark)                                                                                                                                     | Evidence quote                                 | Source                                                            | Verdict               | Overlap |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------|-----------------------|---------|
| 4   | A remote access VPN gives individual hosts or clients remote and secure access to an organization's network.                                       | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 4<br>061 - Network Security::s04::1 | supported (stem gate) | 0.89    |
| 5   | Zero Trust Network Access restricts a user to only the access and permission required to fulfill the role.                                         | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 4<br>061 - Network Security::s04::1 | supported (stem gate) | 0.64    |
| 6   | IDS/IPS detect or prevent network security attacks such as brute force attacks, Denial-of-Service attacks and exploits of network vulnerabilities. | [verbatim slide quote omitted in public build] | 061 - Network Security, slide 4<br>061 - Network Security::s04::1 | supported (stem gate) | 0.86    |

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

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

## PART A - QUESTION 2

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

#### Question:

*Explain how a substitution cipher works and state what serves as its key.*

#### Marking points:

| No. | Point (1 mark)                                                                                         | Evidence quote                                 | Source                                                                        | Verdict               | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | The cipher works by replacing each plaintext letter with a different letter, producing the ciphertext. | [verbatim slide quote omitted in public build] | 031 - Classical Cryptography, slide 4<br>031 - Classical Cryptography::s04::1 | supported             | 0.43<br>LOW |
| 2   | The key is the rule that determines which substitutions are made.                                      | [verbatim slide quote omitted in public build] | 031 - Classical Cryptography, slide 4<br>031 - Classical Cryptography::s04::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: 031 - Classical Cryptography, slide 4*

### A2b - 6 marks - computed - matches lecture slide 15 (standard tableau)

#### Question:

*Decrypt the following ciphertext using the Vigenere cipher with the key CIPHER. Use the standard 26 x 26 Vigenere tableau, writing the key over the message and repeating it as necessary.*

UMRBVVNWVPREQE

#### Answer: SECURELOGINNOW

*The 26 x 26 Vigenere tableau is printed in the question paper.*

#### Working:

Standard 26 x 26 tableau, A=0; key repeated over the ciphertext.

Ciphertext: UMRBVVNWVPREQE

Key: CIPHERCIPHERCI

Letter-by-letter:  $C - K \bmod 26 = P$

U (20) - C ( 2) = 18 -> S

M (12) - I ( 8) = 4 -> E

R (17) - P (15) = 2 -> C

B ( 1) - H ( 7) = 20 -> U

V (21) - E ( 4) = 17 -> R

V (21) - R (17) = 4 -> E

N (13) - C ( 2) = 11 -> L

W (22) - I ( 8) = 14 -> O

V (21) - P (15) = 6 -> G

P (15) - H ( 7) = 8 -> I  
 R (17) - E ( 4) = 13 -> N  
 E ( 4) - R (17) = 13 -> N  
 Q (16) - C ( 2) = 14 -> O  
 E ( 4) - I ( 8) = 22 -> W  
 Plaintext: SECURELOGINNOW

*Suggested marks: 1 mark for the key/table setup; 4 marks for the letter-by-letter working; 1 mark for the complete answer.*

*Confidence: computed - matches lecture slide 15 (standard tableau).*

## PART A - QUESTION 3

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

#### Question:

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

#### Marking points:

| No. | Point (1 mark)                                                                                                                           | Evidence quote                                 | Source                                                               | Verdict               | Overlap |
|-----|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|---------|
| 1   | Attackers can tamper with resources that are essential to 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) | 0.69    |
| 2   | A major cause of software insecurity is the failure to validate user input.                                                              | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 30<br>051 - Software Security::s30::1 | supported (stem gate) | 0.62    |

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

*Citations: 051 - Software Security, slide 30*

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

#### Question:

*Windows is often described as having rich but complicated security. Explain six aspects of Windows security mechanisms, covering how subjects and credentials are handled, how resources are organised and controlled, and why this complexity can itself become a security problem.*

#### Marking points:

| No. | Point (1 mark)                                                                                                                                       | Evidence quote                                 | Source                                                             | Verdict               | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------|-----------------------|-------------|
| 1   | Windows subjects are processes and threads, i.e. active entities in OS primitives.                                                                   | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 11<br>041 - Windows Security::s11::1 | supported (stem gate) | 0.57        |
| 2   | A subject's security credentials are kept in a token, which maps principals to subjects and may carry extra security attributes.                     | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 11<br>041 - Windows Security::s11::1 | partly supported      | 0.36<br>LOW |
| 3   | Active Directory, introduced in Windows 2000, is an LDAP-like directory service used to organise users, groups, credentials, resources and policies. | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 6<br>041 - Windows Security::s06::1  | supported (stem gate) | 0.64        |
| 4   | Windows provides complex mechanisms for user account and object management as well as access control.                                                | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 21<br>041 - Windows Security::s21::1 | supported (stem gate) | 0.91        |
| 5   | Discretionary access control in Windows allows fine-grained control over heterogeneous entities both in the OS and in applications.                  | [verbatim slide quote omitted in public build] | 041 - Windows Security, slide 21<br>041 - Windows Security::s21::1 | supported (stem gate) | 0.58        |
| 6   | The very complexity of these mechanisms is a weakness, since misconfiguration and 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 |

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

Citations: 041 - Windows Security, slide 11; 041 - Windows Security, slide 21; 041 - Windows Security, slide 6

## PART A - QUESTION 4

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

#### Question:

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

#### Marking points:

| No. | Point (1 mark)                                                             | Evidence quote                                 | Source                                                               | Verdict               | Overlap     |
|-----|----------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|-------------|
| 1   | They disguise themselves as useful or benign software.                     | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 12<br>051 - Software Security::s12::1 | supported             | 0.20<br>LOW |
| 2   | They replicate themselves and steal information or damage the host system. | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 12<br>051 - Software Security::s12::1 | supported (stem gate) | 0.75        |

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

Citations: 051 - Software Security, slide 12

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

#### Question:

Discuss six (6) malware attack techniques and propagation behaviours, explaining how each technique or behaviour enables the malware to spread or to act on an infected system.

#### Marking points:

| No. | Point (1 mark)                                                                                                                                              | Evidence quote                                 | Source                                                               | Verdict               | Overlap     |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|-------------|
| 1   | A rootkit hides malicious processes and software so that the infected machine stays under the attacker's remote control after a vulnerability is exploited. | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 13<br>051 - Software Security::s13::1 | supported             | 0.40<br>LOW |
| 2   | Spyware covertly gathers user credentials and activity, for example by logging keystrokes and recording visited sites.                                      | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 13<br>051 - Software Security::s13::1 | supported             | 0.42<br>LOW |
| 3   | 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        |
| 4   | A virus can overwrite the program header so that execution is redirected to the virus code before returning to the original entry point.                    | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 10<br>051 - Software Security::s10::1 | supported             | 0.39<br>LOW |
| 5   | Early self-replicating code spread by infecting the boot sector of distributed diskettes, as the Brain virus did.                                           | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 7<br>051 - Software Security::s07::1  | partly supported      | 0.31<br>LOW |
| 6   | A worm can propagate over a network by exploiting a remote execution feature of a service, as the Morris worm did through sendmail.                         | [verbatim slide quote omitted in public build] | 051 - Software Security, slide 7<br>051 - Software Security::s07::1  | partly supported      | 0.23<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 5

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

*Explain the difference between morals, ethics and laws as sources of guidance for professional conduct in 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, forming the basis of social behaviour. | [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) | 0.55    |
| 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*

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

*State six requirements that a professional code of ethics and conduct places on a computing professional, as illustrated by the ACM code and its professional conduct guidance.*

**Marking points:**

| No. | Point (1 mark)                                                                                                                | Evidence quote                                 | Source                                                                                     | Verdict               | Overlap     |
|-----|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | The professional must contribute to society and human well-being, recognising that all people are stakeholders in computing.  | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 11<br>071 - Ethics and Computer Security::s11::1 | supported (stem gate) | 0.73        |
| 2   | The professional must respect privacy and honour confidentiality in handling information.                                     | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 11<br>071 - Ethics and Computer Security::s11::1 | partly supported      | 0.25<br>LOW |
| 3   | The professional must strive for high quality in both the processes and the products of 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) | 0.89        |
| 4   | The professional must know and respect the existing rules that pertain 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) | 0.88        |
| 5   | The professional must perform work only in areas where he or she is competent.                                                | [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 access computing and communication resources only when authorised or when compelled by the public good. | [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        |

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 12

## PART A - QUESTION 6

### A6a - 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 them. | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 5<br>072 - Biometrics and Authentication::s05::1 | supported             | 0.30<br>LOW |
| 2   | The authentication stage involves further acquisition, comparison against the stored data 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) | 0.50        |

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

Citations: 072 - Biometrics and Authentication, slide 5

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

#### Question:

Explain the categories of biometric applications and the characteristics of iris and fingerprint technologies, including the practical problems associated with fingerprint systems.

#### Marking points:

| No. | Point (1 mark)                                                                              | Evidence quote                                 | Source                                                                                       | Verdict               | Overlap |
|-----|---------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------|---------|
| 1   | Biometric applications are divided into two sectors, namely physiological and behavioural.  | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 4<br>072 - Biometrics and Authentication::s04::1  | supported (stem gate) | 0.57    |
| 2   | The physiological category includes 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    |
| 3   | The behavioural category includes 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    |
| 4   | Iris scanning works by scanning the unique pattern of the iris.                             | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 10<br>072 - Biometrics and Authentication::s10::1 | supported (stem gate) | 0.80    |

| No. | Point (1 mark)                                                                                      | Evidence quote                                 | Source                                                                                       | Verdict          | Overlap     |
|-----|-----------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------------|------------------|-------------|
| 5   | Iris scanning requires no touch and overcomes the issues associated with retinal scanners.          | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 10<br>072 - Biometrics and Authentication::s10::1 | partly supported | 0.22<br>LOW |
| 6   | Fingerprint systems suffer from racial issues, dirt, grime and wounds, and placement of the finger. | [verbatim slide quote omitted in public build] | 072 - Biometrics and Authentication, slide 7<br>072 - Biometrics and Authentication::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: 072 - Biometrics and Authentication, slide 10; 072 - Biometrics and Authentication, slide 4; 072 - Biometrics and Authentication, slide 7*

## PART A - QUESTION 7

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

#### Question:

*State TWO (2) formal security models that are classified as information flow models, and state the specific concern that the Chinese Wall model is designed to address.*

#### Marking points:

| No. | Point (1 mark)                                                                                                         | Evidence quote                                 | Source                                                                       | Verdict               | Overlap |
|-----|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------|-----------------------|---------|
| 1   | The Chinese Wall model is listed as an information flow model, identified by its detection of 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) | 0.62    |
| 2   | The Chinese Wall policy is specifically designed to address conflicts of interest faced by a consultant or contractor. | [verbatim slide quote omitted in public build] | 024 - Formal Security Model, slide 27<br>024 - Formal Security Model::s27::1 | supported (stem gate) | 0.90    |

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

*Citations: 024 - Formal Security Model, slide 27; 024 - Formal Security Model, slide 5*

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

#### Question:

*Describe the access control matrix, the access control list and the capability list as access control structures, giving one advantage and one disadvantage of the access control matrix and of the access control list, and stating what a capability list represents.*

#### Marking points:

| No. | Point (1 mark)                                                                                         | Evidence quote                                 | Source                                                                                            | Verdict   | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------|-------------|
| 1   | The access control matrix is identified 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 |

| No. | Point (1 mark)                                                                                                                                 | Evidence quote                                 | Source                                                                                             | Verdict               | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------------------|-----------------------|-------------|
| 2   | An advantage of the access control matrix is that it is clear to define 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             | 0.38<br>LOW |
| 3   | A disadvantage of the access control matrix is poor scalability and poor handling of changes.                                                  | [verbatim slide quote omitted in public build] | 023 - Access Control and Authorization, slide 8<br>023 - Access Control and Authorization::s08::1  | supported (stem gate) | 0.62        |
| 4   | An access control list is described as 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   | An advantage of the access control list is easy access to an object's access rights and relative easiness of management using abstractions.    | [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) | 0.89        |
| 6   | A disadvantage of the access control list is a poor overview of access rights per subject, difficulty of revocation and difficulty of sharing. | [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) | 0.82        |

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

## PART A - QUESTION 8

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

#### Question:

*Explain two ways in which a documented professional code of ethics shapes the ethical impact of technology practice, as described in the lecture.*

#### Marking points:

| No. | Point (1 mark)                                                                                                                                                                          | Evidence quote                                 | Source                                                                                    | Verdict          | Overlap     |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------|------------------|-------------|
| 1   | A code of ethics is a documented set of acceptable behaviours for a professional or social group, so it sets the standard against which the ethical impact of technology use is judged. | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 6<br>071 - Ethics and Computer Security::s06::1 | partly supported | 0.43<br>LOW |
| 2   | Such a code adds clarity to the understanding of acceptable standards of behaviour, making the ethical expectations of technology work explicit.                                        | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 8<br>071 - Ethics and Computer Security::s08::1 | supported        | 0.36<br>LOW |

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

Citations: 071 - Ethics and Computer Security, slide 6; 071 - Ethics and Computer Security, slide 8

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

#### Question:

Refer to your answer in (a). Discuss how professional codes of ethics and the responsibilities of information specialists address privacy and organisational responsibility in computer security practice.

#### Marking points:

| No. | Point (1 mark)                                                                                                                           | Evidence quote                                 | Source                                                                                    | Verdict               | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Professional bodies such as the ACM publish a code of ethics and professional conduct that members are expected to follow.               | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 7<br>071 - Ethics and Computer Security::s07::1 | partly supported      | 0.36<br>LOW |
| 2   | The ACM has established a code of ethics and professional conduct for computing practitioners.                                           | [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) | 0.78        |
| 3   | Merely describing moral and ethical dimensions of ICT is insufficient; organisations must actively address them.                         | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 3<br>071 - Ethics and Computer Security::s03::1 | partly supported      | 0.36<br>LOW |
| 4   | Users in general carry definite responsibilities to act within ethical, moral and legal constraints.                                     | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 3<br>071 - Ethics and Computer Security::s03::1 | supported (stem gate) | 0.82        |
| 5   | Information specialists in particular bear responsibility for performing within ethical, moral and legal constraints when handling data. | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 3<br>071 - Ethics and Computer Security::s03::1 | supported (stem gate) | 0.71        |
| 6   | Organisational responsibility for privacy is grounded in the ethical, moral and legal constraints that govern how ICT is used.           | [verbatim slide quote omitted in public build] | 071 - Ethics and Computer Security, slide 3<br>071 - Ethics and Computer Security::s03::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.

Citations: 071 - Ethics and Computer Security, slide 3; 071 - Ethics and Computer Security, slide 7

## PART A - QUESTION 9

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

#### Question:

Explain how a disclosure threat and a usurpation threat each affect the confidentiality, integrity and availability of a system's assets.

#### Marking points:

| No. | Point (1 mark)                                                                                                                                                     | Evidence quote                                 | Source                                                                                               | Verdict          | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------|-------------|
| 1   | Disclosure is unauthorised access to information (e.g. snooping, sniffing, wiretapping) and is countered by confidentiality services, so it harms confidentiality. | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 10<br>011 - Introduction to Computer Security::s10::1 | partly supported | 0.27<br>LOW |

| No. | Point (1 mark)                                                                                                                                                                     | Evidence quote                                 | Source                                                                                               | Verdict          | Overlap     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|------------------|-------------|
| 2   | Usurpation is unauthorised control of part of a system (via modification, spoofing, delay, denial of service) and is countered by availability services, so it harms availability. | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 10<br>011 - Introduction to Computer Security::s10::1 | partly supported | 0.29<br>LOW |

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

*Citations: 011 - Introduction to Computer Security, slide 10*

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

#### Question:

*State six (6) characteristics of the Samy worm and the cross-site scripting (XSS) mechanism it exploited, explaining how each characteristic enabled the worm to spread or to act on an infected profile.*

#### 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 field by performing XML-HTTP 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) | 0.78        |
| 4   | Any user visiting an infected user's page had their profile infected with JavaScript and their friends list infected with Samy.                                 | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 15<br>052 - Web Security::s15::1 | supported (stem gate) | 0.80        |
| 5   | The worm scaled to about 1,000,000 infected MySpace profiles.                                                                                                   | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 15<br>052 - Web Security::s15::1 | supported (stem gate) | 0.57        |
| 6   | Any web application that returns user input without filtering is a potential XSS vulnerability, allowing arbitrary JavaScript to execute in the user's browser. | [verbatim slide quote omitted in public build] | 052 - Web Security, slide 13<br>052 - Web Security::s13::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: 052 - Web Security, slide 13; 052 - Web Security, slide 15*

## PART A - QUESTION 10

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

#### Question:

*State TWO (2) detection outcomes that an intrusion detection system may produce when monitoring for attacks, and explain what each outcome indicates about the system's detection accuracy.*

#### Marking points:

| No. | Point (1 mark)                                                                   | Evidence quote                                 | Source                                                                                 | Verdict               | Overlap |
|-----|----------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------|---------|
| 1   | A true positive occurs when the IDS correctly identifies an intrusion or attack. | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 31<br>062 - Intrusion Detection System::s31::1 | supported (stem gate) | 0.50    |

| No. | Point (1 mark)                                                                       | Evidence quote                                 | Source                                                                                 | Verdict               | Overlap |
|-----|--------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------|---------|
| 2   | A false positive is a legitimate activity that the IDS wrongly reports as malicious. | [verbatim slide quote omitted in public build] | 062 - Intrusion Detection System, slide 31<br>062 - Intrusion Detection System::s31::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: 062 - Intrusion Detection System, slide 31*

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

#### Question:

*Discuss six (6) threat classes and countermeasures relevant to computer security, explaining for each how the threat class endangers assets or how the countermeasure addresses it.*

#### Marking points:

| No. | Point (1 mark)                                                                                                                                                                | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap  |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|----------|
| 1   | A threat is described as a potential violation of security rather than an actual one, so it represents a danger that may or may not materialise against an asset.             | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 9<br>011 - Introduction to Computer Security::s09::1  | partly supported      | 0.29 LOW |
| 2   | An attack is distinguished from a threat in that it is the actual violation of security, i.e. the realised exploitation rather than the potential danger.                     | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 9<br>011 - Introduction to Computer Security::s09::1  | partly supported      | 0.33 LOW |
| 3   | A threat is characterised as an object, person or other entity that represents a constant danger to an asset, which is the entity the countermeasures must guard against.     | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 28<br>011 - Introduction to Computer Security::s28::1 | supported (stem gate) | 0.64     |
| 4   | Protection of assets is framed as encompassing prevention, detection and response techniques, giving the three countermeasure categories that can be applied against threats. | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 28<br>011 - Introduction to Computer Security::s28::1 | supported (stem gate) | 0.50     |
| 5   | Forces of nature are treated as among the most dangerous threat classes because they disrupt the storage, transmission and use of information.                                | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 13<br>011 - Introduction to Computer Security::s13::1 | partly supported      | 0.43 LOW |
| 6   | The countermeasure for natural threats is for organisations to implement controls that limit damage and to prepare contingency plans so that operations can continue.         | [verbatim slide quote omitted in public build] | 011 - Introduction to Computer Security, slide 13<br>011 - Introduction to Computer Security::s13::1 | supported (stem gate) | 0.64     |

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

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

*Citations: 011 - Introduction to Computer Security, slide 13; 011 - Introduction to Computer Security, slide 28; 011 - Introduction to Computer Security, slide 9*

## PART B - QUESTION 1

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

#### Question:

*State the role of the TPM in a trusted platform, and explain how a chain of trust is built from the hardware up*

to the running software. Your answer should identify the roots of trust involved and the mechanism used to record each stage.

**Marking points:**

| No. | Point (1 mark)                                                                                                                                                                     | Evidence quote                                 | Source                                                              | Verdict               | Overlap |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------|-----------------------|---------|
| 1   | The TPM is described as a tamper-resistant hardware module mounted in the platform.                                                                                                | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 6<br>073 - Trusted Computing::s06::1 | supported (stem gate) | 1.00    |
| 2   | The TPM is responsible for measurement, protected storage, integrity reporting and policy enforcement.                                                                             | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 6<br>073 - Trusted Computing::s06::1 | supported (stem gate) | 0.89    |
| 3   | In the chain of trust, each stage 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) | 0.50    |
| 4   | The measurements taken at each stage are stored in Platform Configuration Registers (PCRs) on the TPM.                                                                             | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 8<br>073 - Trusted Computing::s08::1 | supported (stem gate) | 0.67    |
| 5   | The Root of Trust for Measurement is the component trusted to reliably measure and report to the Root of Trust for Reporting what software executes at the start of platform boot. | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 7<br>073 - Trusted Computing::s07::1 | supported (stem gate) | 1.00    |

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

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

*Citations: 073 - Trusted Computing, slide 6; 073 - Trusted Computing, slide 7; 073 - Trusted Computing, slide 8*

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

**Question:**

*Discuss the components of the NGSCB architecture, explaining the role of the Nexus and the Nexus Computing Agent and how they work together to protect trusted software from the operating system.*

**Marking points:**

| No. | Point (1 mark)                                                                                                       | Evidence quote                                 | Source                                                               | Verdict               | Overlap     |
|-----|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------|-----------------------|-------------|
| 1   | The Nexus acts as a security kernel that is authenticated during boot.                                               | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 14<br>073 - Trusted Computing::s14::1 | supported (stem gate) | 0.57        |
| 2   | The Nexus authenticates trusted programs and 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 | partly supported      | 0.38<br>LOW |
| 3   | The 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        |
| 4   | The Nexus Computing Agent is a trusted software component that runs in trusted mode and communicates with the Nexus. | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 15<br>073 - Trusted Computing::s15::1 | supported (stem gate) | 0.62        |
| 5   | The Nexus is a special kernel that isolates normal-mode and trusted-mode processes differently in memory.            | [verbatim slide quote omitted in public build] | 073 - Trusted Computing, slide 13<br>073 - Trusted Computing::s13::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).*

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

*Explain five password security controls that an administrator can apply to protect a system's password files and accounts, and state one password policy requirement for the root password.*

**Marking points:**

| No. | Point (1 mark)                                                                          | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap     |
|-----|-----------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|-------------|
| 1   | Apply access control to the password files so that only authorised users can read them. | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 12<br>022 - Identification and Authentication::s12::1 | supported             | 0.36<br>LOW |
| 2   | De-activate an account after several 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) | 0.71        |
| 3   | Show the time of the user's last login so unusual activity can be noticed.              | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 12<br>022 - Identification and Authentication::s12::1 | partly supported      | 0.33<br>LOW |
| 4   | Store the password in an encrypted form using a one-way hash function.                  | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 8<br>022 - Identification and Authentication::s08::1  | supported (stem gate) | 1.00        |
| 5   | For the root password, adopt a policy that it is never divulged over a telephone.       | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 12<br>022 - Identification and Authentication::s12::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: 022 - Identification and Authentication, slide 12; 022 - Identification and Authentication, slide 8*

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

*A company wants to let staff reach many internal services after a single login, using Kerberos and other single sign-on approaches. Explain the motivation for single sign-on, the design criteria that Kerberos aims to satisfy, and the drawbacks of Kerberos that the company should consider.*

**Marking points:**

| No. | Point (1 mark)                                                                                         | Evidence quote                                 | Source                                                                                               | Verdict   | Overlap     |
|-----|--------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------|-------------|
| 1   | Single sign-on reduces the burden on users by cutting down the number of passwords they must remember. | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 16<br>022 - Identification and Authentication::s16::1 | supported | 0.17<br>LOW |

| No. | Point (1 mark)                                                                                           | Evidence quote                                 | Source                                                                                               | Verdict               | Overlap     |
|-----|----------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------|-------------|
| 2   | Single sign-on also lowers the time users spend typing passwords and the effort needed to maintain them. | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 16<br>022 - Identification and Authentication::s16::1 | partly supported      | 0.17<br>LOW |
| 3   | Kerberos is designed to resist eavesdropping by never sending 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             | 0.44<br>LOW |
| 4   | Kerberos aims for transparency, so the user notices no 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) | 0.67        |
| 5   | Kerberos is relatively complex to install and represents a single point of failure.                      | [verbatim slide quote omitted in public build] | 022 - Identification and Authentication, slide 23<br>022 - Identification and Authentication::s23::1 | partly supported      | 0.38<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: 022 - Identification and Authentication, slide 16; 022 - Identification and Authentication, slide 18; 022 - Identification and Authentication, slide 23*

*End of marking scheme.*