

Markscheme

May 2026

Computer science

Higher level

Paper 3

© International Baccalaureate Organization 2026

All rights reserved. No part of this product may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without the prior written permission from the IB. Additionally, the license tied with this product prohibits use of any selected files or extracts from this product. Use by third parties, including but not limited to publishers, private teachers, tutoring or study services, preparatory schools, vendors operating curriculum mapping services or teacher resource digital platforms and app developers, whether fee-covered or not, is prohibited and is a criminal offense.

More information on how to request written permission in the form of a license can be obtained from <https://ibo.org/become-an-ib-school/ib-publishing/licensing/applying-for-a-license/>.

© Organisation du Baccalauréat International 2026

Tous droits réservés. Aucune partie de ce produit ne peut être reproduite sous quelque forme ni par quelque moyen que ce soit, électronique ou mécanique, y compris des systèmes de stockage et de récupération d'informations, sans l'autorisation écrite préalable de l'IB. De plus, la licence associée à ce produit interdit toute utilisation de tout fichier ou extrait sélectionné dans ce produit. L'utilisation par des tiers, y compris, sans toutefois s'y limiter, des éditeurs, des professeurs particuliers, des services de tutorat ou d'aide aux études, des établissements de préparation à l'enseignement supérieur, des fournisseurs de services de planification des programmes d'études, des gestionnaires de plateformes pédagogiques en ligne, et des développeurs d'applications, moyennant paiement ou non, est interdite et constitue une infraction pénale.

Pour plus d'informations sur la procédure à suivre pour obtenir une autorisation écrite sous la forme d'une licence, rendez-vous à l'adresse <https://ibo.org/become-an-ib-school/ib-publishing/licensing/applying-for-a-license/>.

© Organización del Bachillerato Internacional, 2026

Todos los derechos reservados. No se podrá reproducir ninguna parte de este producto de ninguna forma ni por ningún medio electrónico o mecánico, incluidos los sistemas de almacenamiento y recuperación de información, sin la previa autorización por escrito del IB. Además, la licencia vinculada a este producto prohíbe el uso de todo archivo o fragmento seleccionado de este producto. El uso por parte de terceros —lo que incluye, a título enunciativo, editoriales, profesores particulares, servicios de apoyo académico o ayuda para el estudio, colegios preparatorios, desarrolladores de aplicaciones y entidades que presten servicios de planificación curricular u ofrezcan recursos para docentes mediante plataformas digitales—, ya sea incluido en tasas o no, está prohibido y constituye un delito.

En este enlace encontrará más información sobre cómo solicitar una autorización por escrito en forma de licencia: <https://ibo.org/become-an-ib-school/ib-publishing/licensing/applying-for-a-license/>.

Subject details: Computer science HL paper 3 markscheme

Mark allocation

Candidates are required to answer **all** questions. Total 30 marks.

General

A markscheme often has more specific points worthy of a mark than the total allows. This is intentional. Do not award more than the maximum marks allowed for that part of a question.

When deciding upon alternative answers by candidates to those given in the markscheme, consider the following points:

- Each statement worth one point has a separate line and the end is signified by means of a semi-colon (;).
- An alternative answer or wording is indicated in the markscheme by a “/”; either wording can be accepted.
- Words in (...) in the markscheme are not necessary to gain the mark.
- If the candidate’s answer has the same meaning or can be clearly interpreted as being the same as that in the markscheme then award the mark.
- Mark positively. Give candidates credit for what they have achieved and for what they have got correct, rather than penalizing them for what they have not achieved or what they have got wrong.
- Remember that many candidates are writing in a second language; be forgiving of minor linguistic slips. In this subject effective communication is more important than grammatical accuracy.
- Occasionally, a part of a question may require a calculation whose answer is required for subsequent parts. If an error is made in the first part then it should be penalized. However, if the incorrect answer is used correctly in subsequent parts then **follow through** marks should be awarded. Indicate this with “**FT**”.
- Question 4 is marked against markbands. The markbands represent a single holistic criterion applied to the piece of work. Each markband level descriptor corresponds to a number of marks. When assessing with markbands, a “best fit” approach is used, with markers making a judgment about which particular mark to award from the possible range for each level descriptor, according to how well the candidate’s work fits that descriptor.

General guidance

Issue	Guidance
Answering more than the quantity of responses prescribed in the questions	• In the case of an “identify” question read all answers and mark positively up to the maximum marks. Disregard incorrect answers. • In the case of a “describe” question, which asks for a certain number of facts <i>eg</i> “describe two kinds”, mark the first two correct answers. This could include two descriptions, one description and one identification, or two identifications. • In the case of an “explain” question, which asks for a specified number of explanations <i>eg</i> “explain two reasons ...”, mark the first two correct answers. This could include two full explanations, one explanation, one partial explanation <i>etc.</i>

1. (a) **Award [2 max].**
Award [1] identifying an advantage.
Award [1] explaining how/why.

Advantage:

It provides an unbiased/objective assessment of security;
It simulates a realistic external attack;
It tests the organisation's detection and response capabilities;

Explanation:

The tester has no insider knowledge, so they approach the system without assumptions or blind spots;
It replicates the conditions of a genuine attack, giving a more accurate picture of external risk;
It can expose gaps that internal teams miss due to familiarity with the infrastructure;
It tests not just technical defences but also monitoring/alerting systems under realistic conditions.

- (b) **Award [2 max].**
Award [1] for definition.
Award [1] for expansion.

A technique that uses advanced/specific search engine operators to filter search results;
To find publicly exposed sensitive information (e.g. login pages, config files, passwords) / to identify misconfigurations / to gather reconnaissance on a target / to find data, files, or pages indexed by search engines that were not intended to be publicly discoverable.

Accept Google dorking / Google hacking as equivalent terms / Named operators (e.g. site:, filetype:, inurl:) as evidence of the definition mark.

2. (a) **Award [4 max].**
Award [2] + [2].
Award [1] for stating the impact.
Award [1] for expanding on the same.

Larger attack surface / more connected devices provides more entry points to test;
Multiple protocols (WiFi, Bluetooth, RFID) each require different testing approaches;

Safety constraints limit testing / aggressive techniques (e.g. fuzzing, DoS) could disrupt life-critical devices;

Testers must work within stricter boundaries than with standard IT systems;

Device diversity complicates testing / devices run different OS/firmware;
Standard testing tools may not work across all devices;

Limited device access / devices may not support testing agents or have restricted interfaces;
Harder to test than traditional systems;

Sensitive data increases testing scope / devices capture real-time patient data;
Testers must account for data protection regulations (e.g. HIPAA, GDPR);

Scheduling constraints / IoT medical devices are in continuous 24/7 use;
Difficult to find a testing window that minimises disruption to patient care;

Requires specific contingency/response planning / testers must prepare for device failure;
Due to the critical nature of medical devices, any disruption could endanger patients.

- (b) *Award [4 max].*
Award [2] + [2].
Award [1] for stating a consequence.
Award [1] for expanding on it.

Loss of patient trust / negative relationship;
Health information is personal and sensitive, and patients may switch to other healthcare providers;

Legal/regulatory consequences / violation of data protection regulations (e.g. GDPR, HIPAA);
Can result in lawsuits, fines, or sanctions from regulatory bodies;

Financial loss / costs beyond regulatory fines;
Includes compensation to affected patients, breach investigation costs, and investment in new security measures;

Productivity loss / operations may need to be shut down temporarily;
Causes delays in patient care which can endanger lives;

Impacts on patient care / loss of access to medical records / changes to patient data;
Delays or errors in treatment due to unavailable or corrupted patient data;

Risk to patient safety / compromised medical devices (e.g. life support);
Could directly endanger lives if devices malfunction or are tampered with;

Reputational damage / negative media coverage following a breach;
Loss of public confidence, difficulty attracting staff or patients;

Data exposure / sensitive patient records leaked or accessed;
Could lead to identity theft, blackmail, or data sold on the black market.

Note: Do not award marks for defining a data breach.

3. *Award [6 max].*
Award [1] for any valid point up to [6 max].

Identify a vulnerability through code review, fuzzing, or scanning tools (e.g. Metasploit, Immunity Debugger);
Analyse the vulnerability / understand its nature, root cause, and potential impact;
Research existing knowledge / check CVE entries, documentation, or known proof-of-concept code;
Develop the exploit / craft code/payload to trigger the vulnerability (e.g. buffer overflow, injection);
Test in a controlled environment / verify the exploit works reliably without unintended damage;
Refine the exploit / adapt to avoid detection (e.g. IDS/antivirus evasion) and improve reliability;
Deploy against the target / execute the exploit to gain access or escalate privileges.

Note: Accept a worked example (e.g. buffer overflow).

4. Award [12 max].

Please see mark bands as shown in the table on page 9.

Responses may include the following:

Network Scanning

- Definition: probing a network to identify open ports, running services, and OS versions.
- Active scanning sends packets to devices to gather information / passive scanning monitors existing traffic without injecting packets.
- Tools: Nmap.
- Benefit: Identifies vulnerable services, outdated software, and misconfigured devices.
- Risk to MTPH: aggressive active scans could cause instability on sensitive medical IoT devices (e.g. infusion pumps, monitoring equipment).
- Mitigation: use passive scans where possible / schedule active scans during maintenance windows or low-activity periods / target non-critical systems first.

Network Mapping

- Definition: creating a visual representation of network topology, devices, and connections.
- Tools: Zenmap.
- Benefit: identifies legacy systems, poorly segmented networks, and connections between departments.
- Link to MTPH: helps find outdated devices (e.g. X-ray machines running unsupported OS) and reveals how departments are connected (e.g. outpatient billing to radiology).
- Risk to MTPH: the mapping process relies on scanning techniques that carry the same disruption risks as network scanning.
- Mitigation: build maps using passive scan data first / use existing network documentation to supplement.
- Network scanning steps

OSINT (Open Source Intelligence)

- Definition: gathering publicly available information about the target from external sources.
- Sources: staff LinkedIn profiles, hospital procurement records, leaked credential databases, DNS records, job listings revealing technologies used.
- Tools: Maltego, Spiderfoot, Shodan.
- Benefit: least disruptive technique as it requires no interaction with MTPH's internal network / can reveal exposed data, employee information, or misconfigured services with zero risk to hospital operations.
- Limitation: only finds publicly available information, so may miss internal vulnerabilities.
- Risk to MTPH: ethical and regulatory considerations around collecting data about healthcare staff or patients from public sources / must avoid storing personal details unnecessarily.

Comparison and Evaluation Across Techniques

- OSINT is safest for operational continuity as it does not touch the live network.
- Passive network scanning is a middle ground; low disruption but less detail than active scanning.
- Active scanning is the most thorough but highest risk in a hospital setting.
- A combined approach (OSINT first, then passive scanning, then carefully scoped active scanning) balances thoroughness with safety.

- Network mapping supports both scanning and OSINT by providing context for findings.

Link to Penetration Testing Strategies

- Black box testing relies heavily on OSINT and network scanning as the tester has no prior knowledge.
- Grey box testing uses network scanning and mapping more efficiently as the tester has partial knowledge (e.g. credentials, network diagrams).
- White box testing enables comprehensive scanning but risks disruption if conducted on live systems / mitigation: use a controlled lab or digital twin environment.
- A layered approach (black → grey → white) maximises both realism and coverage.

Data Security Considerations

- Accessing live patient data during scanning risks breaches of data protection regulations (e.g. GDPR, HIPAA). Mitigation: use anonymised datasets or synthetic patient records during testing. All gathered data (from scanning, mapping, or OSINT) must be securely stored and disposed of after testing. Formal authorisation and stakeholder awareness must be obtained before any testing.

Real-World Examples

Accept any relevant, well-applied example. Examples may include:

- NHS WannaCry (2017): exploited unpatched Windows systems / disrupted hospital operations / network scanning and mapping could have identified unpatched systems and poor segmentation before the attack.
- University Hospital Düsseldorf: poor segmentation allowed ransomware to spread / network mapping could have identified pivot routes.
- Canadian hospital SQL injection breach: exploited an unprotected web form / OSINT could have identified the exposed form before an attacker did.

Conclusion

A strong conclusion may include:

- No single technique is sufficient on its own. OSINT, network scanning, and network mapping each reveal different types of information and carry different levels of risk. A combined, phased approach starting with the least disruptive technique (OSINT) and progressing to more intrusive methods (active scanning) is the most appropriate strategy for a healthcare environment.
- The critical nature of MTPH's operations means that disruption risk and data security must be prioritised alongside thoroughness of testing. With proper safeguards (scheduling, anonymisation, formal authorisation, use of test environments), these techniques can be used effectively without compromising patient safety or data security.
- MTPH should adopt an ongoing testing cycle rather than a one-off exercise, as new vulnerabilities emerge continuously.

Marks	Level descriptor
No marks	• No knowledge or understanding of the relevant issues and concepts. • No use of appropriate terminology.
Basic 1–3 marks	• Minimal knowledge and understanding of the relevant issues or concepts. • Minimal use of appropriate terminology. • The answer may be little more than a list. • No reference is made to the information in the case study or independent research.
Adequate 4–6 marks	• A descriptive response with limited knowledge and/or understanding of the relevant issues or concepts. • A limited use of appropriate terminology. • There is limited evidence of analysis. • There is evidence that limited research has been undertaken.
Competent 7–9 marks	• A response with knowledge and understanding of the related issues and/or concepts. • A response that uses terminology appropriately in places. • There is some evidence of analysis. • There is evidence that research has been undertaken.
Proficient 10–12 marks	• A response with a detailed knowledge and clear understanding of the computer science. • A response that uses terminology appropriately throughout. • There is competent and balanced analysis. • Conclusions are drawn that are linked to the analysis. • There is clear evidence that extensive research has been undertaken.

[12]