

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] for any correct point.

Identifies vulnerabilities that could be exploited (e.g. ransomware);
Strengthens data security / helps prioritize security/mitigate risks;
Safeguards patient information;
Assesses security of connected medical devices;
Provides assurance to patients through documentation;
Ensures regulatory compliance;
Reduces risk of downtime;
Mitigates risk of insider attacks;
Improves incident response readiness / Improves preparedness for an attack;
Builds stakeholder trust.

Accept any other correct answers.

- (b) *Award [2 max].*
Award [1] for any correct challenge.
Award [1] for expansion.

Potential bias;
which might lead testers to overlook less obvious vulnerabilities;

Overemphasis on internal workings;
may lead to missing some external vulnerabilities;

Security/confidentiality concerns around sharing sensitive data;
exposing code, configurations, and internal documents to testers increases risk;

Time-consuming;
due to the depth and thoroughness of testing required;

May not simulate a realistic external attack;
since testers have full knowledge that real attackers don't/may miss vulnerabilities.

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

Identifying and fixing vulnerabilities (prevention);
Finds weaknesses and provides recommendations to improve security;

Incident response (during an attack);
Helps staff detect, contain, and respond quickly to minimise damage;

Incident recovery / business continuity (after an attack);
Supports restoring systems and resuming operations / reduces downtime;

Compliance and auditing / evidence or proactive security measures;
Demonstrates adherence to regulations (e.g. HIPAA) / provides audit evidence;

Guidance on staff training and awareness needs;
Informs training against threats like phishing.

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

Patient data exposure: testing may risk accessing, damaging, or losing sensitive patient records;
which could be life threatening/risk legal ramifications/extreme consequences;

Disruption to critical care: testing could cause downtime to medical devices or systems providing critical patient support;
this could lead to care disruptions or delayed procedures;

Medical devices: testing devices risks damaging equipment that may be difficult to replace;
careful handling is needed to ensure devices are tested without compromising function;

Scope and authorisation: testing should have clearly defined parameters including which systems, timeframes, and boundaries;
testing without agreed scope risks unintended impact on critical operations.

3. *Award [6 max].*
Award [3] + [3].
Award [1] for stating a concern.
Award [2] for expanding on it.

Increased attack surface: more IoT devices means more entry points for attackers;
devices may use different communication protocols with inadequate security measures, increasing vulnerability;
third-party maintenance providers may not adhere to cybersecurity standards;

Increased data volume: IoT devices continuously monitor patients, generating large amounts of sensitive data;
this data is valuable to cybercriminals, increasing the likelihood of breaches;
many IoT devices do not encrypt data by default, leaving transmitted information vulnerable;

Regulatory compliance: regulations such as HIPAA are slow to keep pace with emerging IoT technologies;
this means devices may be deployed without adequate security guidelines;
leaving hospitals exposed to risks that current frameworks do not address;

Legacy/unpatched devices: many IoT medical devices run outdated operating systems that no longer receive security updates;
manufacturers may not provide firmware patches/there are known vulnerabilities;
leaving known vulnerabilities permanently exploitable;

Lack of network segmentation: IoT devices are often connected to the same network as critical hospital systems;
a compromised device could provide lateral movement across the network;
allowing attackers to access patient records or disrupt other systems.

Accept other reasonable risks.

4. Award [12 max].

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

Students may discuss the following points:

Techniques

- Implement penetration testing techniques.
- Schedule scans when system updates happen.
- Apply software patches to address known risks.
- Back up critical data and have a data recovery plan.
- Automate testing to reduce time and effort for repetitive tasks.
- Conduct regular cybersecurity training for employees.
- Include cybersecurity requirements in vendor contracts.
- Vulnerability scanning for known CVEs.

Protecting and maintaining operational continuity

- Authentication and access control: Prevents unauthorized access, implementation is complex, users may resist changes.
- Data encryption: Keeps patient data from being used by cybercriminals.
- Network security: Firewalls, network segmentation, IDS/IPS, network mapping and scanning.
- Regular penetration testing/risk assessment: Helps respond proactively, reduces incident response time, and helps comply with regulatory requirements like HIPAA.
- Advanced threat detection: Detects unusual patterns and potential threats, giving an early warning of cyberattacks. Accept SIEM, behavioural analytics.
- Defence in depth: No single solution is sufficient; a layered security approach is needed.

Response strategies

- Create a response plan to minimize disruption and the cost of a cyberattack.
- Attack surface management: Continuously scan and identify hardware, software and cloud assets for weak points/entry points for cyberattacks.
- Remediation and monitoring: Use behavioural analytics and machine learning algorithms to identify abnormal user and device behaviour that may indicate a security breach.
- Develop and regularly update a response plan that ensures the organization is prepared to respond quickly and effectively. Ensure that staff are familiar with the procedures through regular drills and tabletop exercises.
- Forensic analysis: Preserve evidence post-incident to understand how the breach occurred and prevent recurrence.
- Communication plan: Notifying patients, regulators, and stakeholders after a breach.

Conclusions

- For early detection and containment of attacks, proper system configuration and maintenance are critical. However, misconfigurations can lead to vulnerabilities, and managing segmented networks can be complex.
- Maintaining ongoing training programmes can be challenging, as it requires continuous effort and trained personnel and is resource intensive.
- Developing and regularly updating the response plan requires effort. Regular drills can be resource intensive.
- There is a risk of false positives and alert fatigue.

- Assessing and managing third-party risks can be complex and time-consuming. Ensuring vendors comply with security standards requires ongoing effort.
- Some vulnerabilities can be missed even with the best efforts.
- Balancing security investment against hospital budgets requires careful cost-benefit analysis.

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.