

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 up to [2 max].*
Award [1] for any topology.

Bus;
Star;
Ring;
Mesh;
Tree (hierarchical);
Hybrid;
Point-to-point;
Daisy chain;
Etc...

- (b) *Award [2 max].*
Award [1] for identifying a limit.
Award [1] for its associated outline.

Time restrictions / testing may be limited to specific hours;
to avoid disrupting normal operations (e.g. outside business hours);

Test intensity / aggressive techniques such as denial-of-service attacks may be prohibited;
to prevent system crashes or downtime to live services;

Data sensitivity / testers may be prohibited from accessing or exfiltrating sensitive data;
to protect personal records, financial information or intellectual property;

Physical access restrictions / certain physical locations such as server rooms may be designated off-limits;
to prevent accidental damage or security risks to critical infrastructure;

Scope of vulnerability testing / testing may be restricted to specific vulnerability types (e.g. web application only);
to keep the engagement focused and manageable within the agreed objectives;

Network traffic limits / testers may be restricted from generating excessive network traffic;
to prevent degradation of live services for end users;

Social engineering restrictions / tactics such as phishing or impersonation of staff may be excluded;
to avoid causing distress or confusion among employees;

Tool and exploit restrictions / the use of destructive tools or zero-day exploits may be prohibited;
to prevent irreversible damage to production systems;

Budget or resource constraints / testing scope may be reduced to fit within an agreed budget;
to limit the number of systems tested or days of engagement;

Departmental exclusions / specific departments or critical systems may be excluded from testing;
to avoid risk to essential services such as live medical equipment or trading platforms.

Accept any other valid limit and associated outline.

2. (a) **Award [4 max].**
Award benefit [2] + limitation [2].
Award [1] for identifying a benefit / limitation.
Award [1] for its associated outline.

Benefits

Cost-effective / utilises publicly available resources;
reducing the need for expensive tools or paid services;

Legal and ethical / gathers information from publicly accessible sources;
minimising the legal risks associated with data collection compared to active reconnaissance;

Non-intrusive / doesn't require direct interaction with the target system;
reducing the chance of detection by the target organisation;

Broad information scope / provides access to a wide range of data sources such as websites, social media and public databases;
allowing testers to build a comprehensive profile of the target;

Real-time data / can gather up-to-date information;
allowing for dynamic analysis of the target's current security posture rather than relying on outdated records;

Low risk of disruption / collecting open-source information doesn't interact with the target's network;
meaning there is no risk of causing downtime or system instability;

Initial vulnerability identification / helps identify basic vulnerabilities and potential attack vectors;
before committing resources to deeper and more intrusive testing phases;

Supports threat modelling / offers insights into the target's external presence;
helping to prioritise potential threats and weaknesses for later testing phases;

Limitations:

Data overload / the vast amount of publicly available data can lead to information overload;
making it difficult and time-consuming to filter and extract relevant insights;

Data accuracy / publicly available information may be outdated, inaccurate or deliberately falsified; which can lead to unreliable conclusions and wasted testing effort;

Limited scope / OSINT is restricted to publicly accessible information; meaning internal configurations, private networks and sensitive data remain out of reach;

Time-consuming / manually searching through open-source data can be time-intensive; especially when filtering large volumes of irrelevant information for useful intelligence;

Detection risk / some OSINT activities such as repeated access to specific forums or social media profiles; might alert the target organisation if conducted carelessly;

Lack of context / OSINT may reveal surface-level data but often lacks depth; making it harder to fully understand the significance or exploitability of discovered information;

Ethical and privacy concerns / gathering personal information from social media or public sources can raise ethical issues; even if the data is technically publicly available (e.g. employee personal details);

Legal constraints / some jurisdictions may have legal restrictions on certain types of public data collection; potentially limiting the scope and effectiveness of OSINT in those regions;

Difficulty verifying source credibility / determining the reliability of OSINT sources can be challenging; leading to potential misinterpretation of data and flawed testing decisions;

Incomplete picture / OSINT focuses only on publicly available data; providing only a partial view of the target's security posture and potentially missing critical internal vulnerabilities;

Accept any other valid benefit/limitation and associated outline.

(b) *Award up to [4 max].*

Award [1] for any correct point up to [4 max].

Define the network range (IP addresses or subnets) to be scanned;

Perform a ping sweep to discover which devices are active on the network;

Conduct port scanning to identify open ports on the active hosts;

Detect the services running on open ports and gather version information;

Use OS fingerprinting to determine the operating system on each host;

Identify the network's structure including routers, switches and device connections;

Use of specific tools such as Nmap or Nessus to carry out scanning activities;

Compare identified services and OS versions against known vulnerabilities;

Document and record findings for use in later phases of the PTES process;

Analyse the findings to assess the network's exposure and prioritise areas for further testing.

Award [1] for a list taken directly from the case study. i.e. "port scanning, OS detection, and network topology mapping... IP addresses of all devices on the hospital's network are catalogued for a comprehensive understanding of the network's scope.

3. *Award [6 max].*
Award [3] + [3].

Comprehensive coverage / automated tools quickly scan large networks for known vulnerabilities;
manual techniques can investigate complex or subtle security issues that require human expertise,
providing a more complete analysis than either approach alone;

Prioritisation of remediation / automated tools generate large lists of vulnerabilities without distinguishing urgency;
manual analysis allows testers to rank findings by severity and business impact;
helping the organisation address the most critical issues first;

Efficiency / automated tools speed up the process by handling large volumes of data across the network;
allowing manual testing to focus on the most critical or high-risk areas;
making the overall vulnerability analysis more time-efficient;

Reduced false positives / automated tools may flag vulnerabilities that are not genuine threats;
manual techniques can verify these results to confirm whether they are real;
ensuring that only accurately identified vulnerabilities are prioritised and reducing unnecessary remediation work;

Contextual analysis / automated tools may identify vulnerabilities without understanding their significance to a specific system;
manual techniques allow human testers to assess the actual risk and impact within the hospital environment;
such as whether a vulnerability directly affects patient safety or critical operations;

Scalability / automated tools are effective for scanning large and complex infrastructures quickly;
while manual techniques allow for targeted deep-dive analysis in high-risk areas;
making the combined process scalable to networks of varying size and complexity;

Cost-effectiveness / automating routine scanning tasks reduces the time and labour costs associated with vulnerability analysis;
while reserving manual techniques for critical or high-value areas;
optimising resource allocation within the testing budget;

Adaptability / automated tools rely on known vulnerability databases and may struggle with unique or novel threats;
manual techniques can adapt to custom systems, configurations or emerging vulnerabilities;
providing greater flexibility when dealing with threats that have no existing signatures;

Detection of zero-day vulnerabilities / automated tools depend on pre-existing databases and cannot identify unknown flaws;
manual techniques allow testers to use creative and exploratory methods;
to discover previously unknown vulnerabilities that have no existing patches or documented fixes;

Deeper exploitation testing / automated tools can identify surface-level vulnerabilities but cannot chain multiple weaknesses together;
manual techniques allow testers to explore how combining several minor vulnerabilities could lead to a significant breach;
providing a more realistic assessment of how an actual attacker might exploit the network.

4. Award [12 max].

Please see mark bands as shown in the table on page 12.

The answer could include the following:

Importance of a comprehensive response plan

- Helps manage and mitigate cybersecurity incidents; ensures quick identification, containment and resolution of threats, reducing potential harm to hospital operations and patient data.
- A combined proactive and reactive approach provides defence in depth; proactive measures aim to prevent incidents while reactive measures ensure the organisation can respond effectively when incidents occur.
- Minimises financial and reputational damage; effective incident response reduces costs associated with breaches (e.g. legal fees, fines, compensation) and maintains public trust in the hospital.

Proactive measures (PTES)

The penetration testing execution standard (PTES) provides a structured and proactive framework for testing security systems before incidents occur:

- Pre-engagement interactions; aligns penetration testing goals with hospital operations, ensuring that testing is thorough but non-disruptive to critical services.
- Intelligence gathering; OSINT techniques help to identify vulnerabilities from external sources before exploitation by real attackers, for example examining staff social profiles could reveal system usage habits, software details or weak security practices.
- Threat modelling; identifies potential attackers and key hospital systems (e.g. EHRs, IoT-enabled devices) that are most at risk, allowing the hospital to focus resources on protecting the most valuable assets.
- Vulnerability analysis; finds weaknesses proactively, allowing for timely remediation before attacks occur.
- Exploitation testing; demonstrates the feasibility of attacks and helps develop tailored defensive strategies.
- Post-exploitation and reporting; assesses impacts of vulnerabilities and informs the hospital on how to respond to breaches if they occur.

Reactive measures

- Incident detection; continuously monitor network activities for signs of intrusion or unusual behaviour, enabling early identification of threats before they escalate.
- Response strategy; plan for containment of breaches, patching of vulnerabilities and stopping data theft or corruption.
- Recovery processes; restore systems to operational state while maintaining data integrity and continuity of services.
- Backup and disaster recovery; ensure regular backups of critical data such as EHRs so that systems can be restored after a ransomware attack or data corruption, minimising downtime.
- Forensic analysis; after incidents, analyse breaches to prevent recurrence and improve future defences.
- Communication plan; notify stakeholders (e.g. patients, regulators) and coordinate with law enforcement if required, ensuring transparency and compliance.
- Role assignment and escalation procedures; define clear responsibilities and chains of command during an incident so that staff know who to contact and what actions to take at each stage.

Healthcare environment specifics

- Patient data protection; sensitive medical records are high-value targets and securing these ensures compliance with data privacy laws and protects patient confidentiality.
- Uninterrupted service delivery; hospitals rely on connected devices for critical care, and a comprehensive plan mitigates risks of service disruption (e.g. IoT-enabled medical devices).
- Regulatory compliance; adhering to healthcare regulations (e.g. HIPAA, GDPR) ensures the hospital avoids penalties and maintains operational legitimacy.

Ethical and operational considerations

- Non-disruption of services; during proactive measures like penetration testing, critical services should remain unaffected to ensure patient safety.
- Data confidentiality; ensuring any testing and subsequent incident response does not compromise patient data integrity.
- Ethical testing boundaries; penetration testing must avoid exploiting vulnerabilities in ways that could harm patients (e.g. tampering with medical devices).

Ongoing preparedness

- Staff training and awareness; hospital staff should be trained to recognise and respond to threats such as phishing, vishing and social engineering attacks, as untrained employees are often the weakest link in cybersecurity;
- Regular testing and review; the response plan should be regularly updated and retested to remain effective against evolving threats, ensuring it does not become outdated;
- Third-party coordination; hospitals rely on external vendors for IoT devices and software, and the response plan should address supply chain risks and coordination with third-party providers during incidents.

Compliance with standards

- Aligning with PTES and industry best practices ensures that both proactive and reactive measures are in line with internationally recognized security standards.
- Integration with other frameworks: Incorporating standards like NIST or ISO 27001 alongside PTES strengthens the hospital's overall cybersecurity posture.

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]