Cambridge Technicals

IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT

05839 - 05842 & 05877

Mark Scheme for June 2025

OCR (Oxford Cambridge and RSA) is a leading UK awarding body, providing a wide range of qualifications to meet the needs of candidates of all ages and abilities. OCR qualifications include AS/A Levels, Diplomas, GCSEs, Cambridge Nationals, Cambridge Technicals, Functional Skills, Key Skills, Entry Level qualifications, NVQs and vocational qualifications in areas such as IT, business, languages, teaching/training, administration and secretarial skills.

It is also responsible for developing new specifications to meet national requirements and the needs of students and teachers. OCR is a not-for-profit organisation; any surplus made is invested back into the establishment to help towards the development of qualifications and support, which keep pace with the changing needs of today's society.

This mark scheme is published as an aid to teachers and students, to indicate the requirements of the examination. It shows the basis on which marks were awarded by examiners. It does not indicate the details of the discussions which took place at an examiners' meeting before marking commenced.

All examiners are instructed that alternative correct answers and unexpected approaches in candidates' scripts must be given marks that fairly reflect the relevant knowledge and skills demonstrated.

Mark schemes should be read in conjunction with the published question papers and the report on the examination.

MARKING INSTRUCTIONS

PREPARATION FOR MARKING
RM ASSESSOR

1. Make sure that you have accessed and completed the relevant training packages for on-screen marking: *RM Assessor Online Training: OCR Essential Guide to Marking*.

2. Make sure that you have read and understood the mark scheme and the question paper for this unit. These are available in RM Assessor

3. Log-in to RM Assessor and mark the **required number** of practice responses ("scripts") and the **required number** of standardisation responses.

MARKING

1. Mark strictly to the mark scheme.

2. Marks awarded must relate directly to the marking criteria.

3. The schedule of dates is very important. It is essential that you meet the RM Assessor 50% and 100% (traditional 40% Batch 1 and 100% Batch 2) deadlines. If you experience problems, you must contact your Team Leader (Supervisor) without delay.

4. If you are in any doubt about applying the mark scheme, consult your Team Leader by telephone, email or via the RM Assessor messaging system.

5. **Crossed-Out Responses**
   Where a candidate has crossed out a response and provided a clear alternative then the crossed-out response is not marked. Where no alternative response has been provided, examiners may give candidates the benefit of the doubt and mark the crossed-out response where legible.

   Contradictory Responses
   When a candidate provides contradictory responses, then no mark should be awarded, even if one of the answers is correct.

Short Answer Questions (requiring only a list by way of a response, usually worth only one mark per response)
Where candidates are required to provide a set number of short answer responses then only the set number of responses should be marked. The response space should be marked from left to right on each line and then line by line until the required number of responses have been considered. The remaining responses should not then be marked. Examiners will have to apply judgement as to whether a 'second response' on a line is a development of the 'first response', rather than a separate, discrete response. *(The underlying assumption is that the candidate is attempting to hedge their bets and therefore getting undue benefit rather than engaging with the question and giving the most relevant/correct responses.)*

Short Answer Questions (requiring a more developed response, worth two or more marks)
If the candidates are required to provide a description of, say, three items or factors and four items or factors are provided, then mark on a similar basis – that is downwards (as it is unlikely in this situation that a candidate will provide more than one response in each section of the response space).

Longer Answer Questions (requiring a developed response)
Where candidates have provided two (or more) responses to a medium or high tariff question which only required a single (developed) response and not crossed out the first response, then only the first response should be marked. Examiners will need to apply professional judgement as to whether the second (or a subsequent) response is a 'new start' or simply a poorly expressed continuation of the first response.

6. Always check the pages (and additional objects if present) at the end of the response in case any answers have been continued there. If the candidate has continued an answer there, then add the annotation 'SEEN' to confirm that the work has been seen and mark any responses using the annotations in section 11.

7. There is a NR (**No Response**) option. Award NR (No Response):

   - if there is nothing written at all in the answer space
   - OR if there is a comment which does not in any way relate to the question (e.g., 'can't do', 'don't know')
   - OR if there is a mark (e.g., a dash, a question mark) which is not an attempt at the question.

   Note: Award 0 marks – for an attempt that earns no credit (including copying out the question).

8. The RM Assessor **comments box** is used by your Team Leader to explain the marking of the practice responses. Please refer to these comments when checking your practice responses. **Do not use the comments box for any other reason.**

9. *Assistant Examiners will send a brief report on the performance of candidates to their Team Leader (Supervisor) via email by the end of the marking period. The report should contain notes on particular strengths displayed as well as common errors or weaknesses. Constructive criticism of the question paper/mark scheme is also appreciated.*

10. For answers marked by levels of response:
To determine the level – start at the highest level and work down until you reach the level that matches the answer
To determine the mark within the level, consider the following

Descriptor	Award mark
On the borderline of this level and the one below	At bottom of level
Just enough achievement on balance for this level	Above bottom and either below middle or at middle of level (depending on number of marks available)
Meets the criteria but with some slight inconsistency	Above middle and either below top of level or at middle of level (depending on number of marks available)
Consistently meets the criteria for this level	At top of level

11. Abbreviations, annotations and conventions used in the detailed Mark Scheme (to include abbreviations and subject-specific conventions).

Annotation	Meaning	Annotation	Meaning
		MAX	Max
BP	Blank Page	NAQ	Not answered question
λ	Omission	NBOD	Benefit of doubt NOT given
✖	Cross	REP	Repeat
	Highlight	SEEN	Seen, Noted but no credit given
I	Ignore	TV	Too vague
L1	Level 1	✓	Tick
L2	Level 2		
L3	Level 3		

12. **Subject-specific Marking Instructions**

INTRODUCTION

Your first task as an Examiner is to become thoroughly familiar with the material on which the examination depends. This material includes:

- the specification, especially the assessment objectives
- the question paper
- the mark scheme.

You should ensure that you have copies of these materials.

You should ensure also that you are familiar with the administrative procedures related to the marking process. These are set out in the OCR booklet **Instructions for Examiners**. If you are examining for the first time, please read carefully **Appendix 5 Introduction to Script Marking: Notes for New Examiners**.

Please ask for help or guidance whenever you need it. Your first point of contact is your Team Leader.

Question			Answer	Marks	Guidance
1	a		• Cyber Criminal (1) • Phisher (1)	2	CAO If three ticks, max 1 If four or more ticks 0 marks Allow indication of choice other than tick
	b		1 from, two marks: • Works within/inside PH Software/employee (1) • Has authorised access to resources (1)	2	
	c		Two from: • Financial gain / money /income generation (1) • Score settling/revenge (1) • Righting perceived wrongs (1)	2	Only allow an answer from these three. Not personal gain
2	a		Two from, 2 marks each: • To recoup the costs of their development investment (1) as the only reseller (1) • To prevent other companies selling the software as their own (1) at a cheaper price/get to market sooner (1) • So that hackers cannot examine it (1) and find any security holes they can exploit (1) • To prevent it being changed / virus added (1) which can infect customers / end user machines (1) • Prevent loss of Intellectual property (1) and loss of sales (1) • Any other valid suggestion	4	NOT DPA/GDPR Allow reverse – what would happen if the code was released. Not reputational damage / loss of trust

	b		3 from, 2 marks each: • Copy (1) to USB stick (1) • Print out (1) and take the physical documents away (1) • Photograph the screen (1) with the documents on (1) • Stand behind another employee / shouldering (1) and note/see what is on the screen (1) • Email (1) to personal email account (1) • Phishing (1) to gather credentials (1) • Escalation of privileges (1) access information their own account cannot get to (1) • Malware (1) installed to gain information / access (1) • Taking printed copy/bin diving (1) with information on it (1) • Eavesdropping (1) collecting/reassembling data in transit (1) • Using a computer an employee has not signed out of (1) and accessing information (1) • Any other valid suggestion	6	It must be a method an insider could use. Malware – allow examples (credit once only) For phishing – NOT sensitive info/access etc, MUST be password / credentials (log in details) NOT just username Phishing / vishing / smishing – allow once1 Hacking – TV Social engineering is TV

	c		Two from, two marks each: • Rival company knows who to contact (1) can put a marketing campaign together specifically against PH software (1) • Customers might leave PH software (1) as their security has been compromised (1) • Reduction in customers (1) can lead to less income / redundancies (1) • Employees might leave (1) as a result of their data being breached (1) • Reputational damage/loss of trust (1) difficult to get new customers / employees (1) • Financial loss (1) through loss of sales / R&D costs (1) • Breach of GDPR (1) fines by ICO (1) • Any other valid suggestion	4	The impact is to PH Software NOT the client/customer/employee

	d		Two from: • Can look at system logs (1) • Can reprint documents (1) • Look at CCTV to see what was on the screen (1) • Lower quotes from competitor (1) • Check insider emails (1) • Similarity in appearance/function of competitors software (1) • Any other valid suggestion	2	Allow Logs on its own NOT missing or deleted data NOT use an IDS/IPS

<table>
<tr>
<td></td>
<td>e</td>
<td></td>
<td>Indicative content may include:

• What worked and what did not when searching for / finding / blocking the insider attack
• How they found out and any patterns that can be applied to find other insiders
• What data can be used to identify trends to uncover potential insider attacks
• Update of documentation, procedures and controls to assist in the investigation focusing on what has worked – so not wasting time on things that do not provide results
• Look at contact list – uptodate / right people notified when running the plan
• Recommend changes to current practices to mitigate future insider attacks

Notes:
This is about how the incident can be used – what lessons can be learnt and how can these lessons be implemented in the prevention of future attacks. Generic answers such as train staff, employ more staff, improve security are NAQ UNLESS they are shown how they are related to lessons learnt from the current incident.</td>
<td>10</td>
<td>
<table>
<tr><td>7 -10 marks</td><td>Candidate has shown a detailed level of understanding by discussing how PH Software can use the incident to assist in its future management of cyber incidents.
Relevant examples will be used to support discussion and ideas will be expressed clearly and fluently.
Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</td></tr>
<tr><td>4-6 marks</td><td>Candidate has shown a good level of understanding by describing how PH Software can use the incident to assist in its future management of cyber incidents.
Some example(s) will be used to support explanations which may not be relevant and may at times detract from the fluency of narrative.
At the bottom of the mark band the candidate may have described (a single) impact.</td></tr>
<tr><td>1 – 3 marks</td><td>Candidate has identified point(s) relevant to how PH Software can use the incident to assist in its future management of cyber incidents.
Limited use of examples to accompany description and ideas will be poorly expressed.
At the bottom of the mark band, (a single) action/impact may be identified with an example.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>Evaluate the effectiveness of an IDS for preventing insider attacks.

Indicative content may include:
• Can alert the network team if any risks and threats are identified allowing them to focus on them to remove/eradicate them
• Inspects the data in packets automatically meaning that the network team does not have to do it manually so a lot more data can be analysed increasing the chances of finding at attack
• Allows the company to meet key legal requirements – the log can be used to show how PH software is conforming.

• Does not block or prevent an attack – just reports/uncovers them. The network manager needs to respond
• Is one tool in the wider management of network security – needs to be paired with other tools to be effective in stopping attacks
• Insider already has access so will not identify them
• Can give false positives – time wasted by the network team on incidents which are non threatening</td>
<td>7</td>
<td>
<table>
<tr><td>5 - 7 marks</td><td>Candidate has evaluated the use of an IDS. Both positive and negative benefits of the use of an IDS have been analysed and the candidate is able to make informed and appropriate judgements within the context provided. An implied conclusion is present which is informed by the supporting analysis.

Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</td></tr>
<tr><td>3 – 4 marks</td><td>Candidate has described the use of an IDS. Positive OR negative benefits of using an IDS have been described and the candidate is able to make some judgements within the context provided.

Some subject specific terminology and knowledge will be used.</td></tr>
<tr><td>1 – 2 marks</td><td>Candidate has identified benefits (positive OR negative) of an IDS

At the bottom of the mark band the candidate may have simply provided a single point about what an IDS does.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table>
</td>
</tr>
</table>

4	**a**	**i**	• Data is accessible when it is needed (1)	1	Allow answers related to when the user wants it, on demand/whenever needed.
		ii	One from: • Data is kept secure (1) • Only accessed by those who need it/authorised (1)	1	Allow private / protected DNA Safe
		iii	One from: • Accuracy (1) • Completeness (1) • Consistent (1) • Valid (1) • Trustworthy (1) • Not tampered with (1) • Up to date (1)	1	
	b		Three from: • Cannot pay any of their bills /go broke (1) • Direct debits can be set up (for loan) (1) • Bad credit record for defaulting on payment (1) • Items they have spent on can be made public embarrassing them/blackmail (1) • Financial loss /money loss (1) • Can be sold to other criminals (1) • Account lockout (1) • Identity Theft (1)	3	Must be financial related Must be a risk to Ryan Not theft on its own

<table>
<tr><td>5</td><td>a</td><td></td><td>4 from:
They did not have authorisation (1) to logon the account (1)
They had unauthorised access (1) to the bank account data / with intent to commit further crime, such as buy goods (1)
The first principle is “unauthorised access to computer material” (1) which they have broken (1)
Any other valid suggestion</td><td>4</td><td>Inappropriate, illegal, unlawful, malicious are TV</td></tr>
<tr><td></td><td>b</td><td>i</td><td>GDPR / DPA / Data Protection (1)</td><td>1</td><td>Date not required</td></tr>
<tr><td></td><td></td><td>ii</td><td>Two from:
Data has not been held securely/failed to protect (1)
Data has been accessed by unauthorised people (1)
Not being used for the purpose for which it was collected (1)</td><td>2</td><td></td></tr>
<tr><td>6</td><td>a</td><td></td><td>One mark for each correct box:<table><tr><th>Method</th><th>Description</th></tr><tr><td>Biometric Access</td><td>Use of a body part (allow example) to gain access</td></tr><tr><td>Patch</td><td>Applying an update to software to close a security vulnerability</td></tr><tr><td>Firewall</td><td>Restricts traffic in and out of the system / applies rules to the data to filter it</td></tr><tr><td>Backup</td><td>Copy of data offsite/external</td></tr><tr><td>Lock / Cable Lock</td><td>Physically connect a computer to a desk to prevent theft</td></tr></table></td><td>5</td><td>Not updates
Firewall – needs monitors and filters
Backup – not just a copy -some reference to stored elsewhere</td></tr>
</table>

	b		Method: • Encryption (1) Two from: • Scrambles it (1) which makes it meaningless (1) • Applies algorithm/key (1) to the plain text (1) • Can only be understood (1) with the key (1) Method: • Packet switching (1) Two from: • Fragments/breaks up data (1) only part of the data can be read if intercepted (1) • Data travels independent routes (1) if one is compromised only part of the data will be read (1)	3	1 for method 2 for how it keeps safe. Marks can be awarded for the second part if they do not mention encryption Read the whole answer awarding credit where it is found Do not accept unreadable for encryption.

Need to get in touch?

If you ever have any questions about OCR qualifications or services (including administration, logistics and teaching) please feel free to get in touch with our customer support centre.

Call us on

01223 553998

Alternatively, you can email us on

support@ocr.org.uk

For more information visit

ocr.org.uk/qualifications/resource-finder

ocr.org.uk

Twitter/ocrexams

/ocrexams

/company/ocr

/ocrexams

CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT

OCR is part of Cambridge University Press & Assessment, a department of the University of Cambridge.

OCR operates academic and vocational qualifications regulated by Ofqual, Qualifications Wales and CCEA as listed in their qualifications registers including A Levels, GCSEs, Cambridge Technicals and Cambridge Nationals.

OCR provides resources to help you deliver our qualifications. These resources do not represent any particular teaching method we expect you to use. We update our resources regularly and aim to make sure content is accurate but please check the OCR website so that you have the most up-to-date version. OCR cannot be held responsible for any errors or omissions in these resources.

Though we make every effort to check our resources, there may be contradictions between published support and the specification, so it is important that you always use information in the latest specification. We indicate any specification changes within the document itself, change the version number and provide a summary of the changes. If you do notice a discrepancy between the specification and a resource, please contact us.

Whether you already offer OCR qualifications, are new to OCR or are thinking about switching, you can request more information using our Expression of Interest form.

Please get in touch if you want to discuss the accessibility of resources we offer to support you in delivering our qualifications.