

Cambridge Technicals IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT
05839 - 05842 & 05877

Mark Scheme for January 2024

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.

© OCR 2024

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 posted on the RM Cambridge Assessment Support Portal <http://www.rm.com/support/ca>
3. Log-in to RM Assessor and mark the **required number** of practice responses (“scripts”) and the **number of required** standardisation responses.

YOU MUST MARK 5 PRACTICE AND 10 STANDARDISATION RESPONSES BEFORE YOU CAN BE APPROVED TO MARK LIVE SCRIPTS.

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 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 or by email.
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.

Multiple Choice Question Responses

When a multiple-choice question has only a single, correct response and a candidate provides two responses (even if one of these responses is correct), then no mark should be awarded (as it is not possible to determine which was the first response selected by the candidate).

When a question requires candidates to select more than one option/multiple options, then local marking arrangements need to ensure consistency of approach.

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 lined pages 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 an annotation to confirm that the work has been seen.
7. Award No Response (NR) if:
 - there is nothing written in the answer spaceAward Zero '0' if:
 - anything is written in the answer space and is not worthy of credit (this includes text and symbols).

8. If you have any questions or comments for your team leader, use the phone, the RM Assessor messaging system, or e-mail.
















9. Assistant Examiners will email a brief report on the performance of candidates to your Team Leader (Supervisor) by the end of the marking period. Your report should contain notes on particular strength 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
	Benefit of Doubt		Max
	Blank Page		Not answered question
	Omission		Benefit of doubt NOT given
	Cross		Repeat
	Highlight		Seen, Noted but no credit given
	Ignore		Too vague
	Level 1		Tick
	Level 2		
	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)	(i)	Three from, e.g.: <ul style="list-style-type: none"> To prevent new challenges (1) being found out by its competition (1) and getting to market first (1) To prevent its financial data being released (1) such as how much it makes per challenge (1) to prevent customers wanting challenges for less money (1) 	3	This is organisational data NOT personal data Not reputation loss
		(ii)	Three from, e.g.: <ul style="list-style-type: none"> Horizontal or vertical (1) gaining access to an account linked to another individual (1) who has the customer list (1) Gain access to other areas of the network (1) their account does not have (1) e.g. financial (1) Targeting a user account that has information you want (1) e.g. by shoulder surfing (1) and finding out their password (1) 	3	Max 2 without an example
	(b)	(i)	Three from, 1 mark each, e.g.: <ul style="list-style-type: none"> Exploiting a bug in the software (1) Shoulder surfing and identifying the password (1) Copying files onto a USB stick (1) Removing printouts from the bin (1) Installing a packet sniffer on the network (1) Photographs of the screen (1) 	3	Must be methods an insider could use. Must be a way and not just a single word NOT Phishing, hacking
		(ii)	Two from, 2 marks each, e.g.: <ul style="list-style-type: none"> Home location can be found out from the data (1) and house can be robbed (1) If customer runs at the same time every day (1) house will be empty and can be robbed (1) If customer runs the same route (1) can be mugged as location known (1) 	4	MUST be safety NOT identity theft / fraud

Question	Answer	Marks	Guidance	
	<p>(iii)* Indicative content may include:</p> <ul style="list-style-type: none"> Confidentiality of data being lost leads to fines under GDPR which can affect the reputation. Customers may leave to a new firm which reduces revenue and long-term viability of the company. Integrity of information may be compromised, such as email addresses altered or payment information changed so that PH cannot contact customers about new challenges or take money from them – affect their ability to sustain the company or pay staff. Availability of information including the website and ability to upload exercise may mean customers lose confidence and move away with financial consequences. <p>Must be for PH and NOT for the customer</p>	10	7-10 marks	<p>Candidate has discussed the impact of the loss of data for PH. Negative explanations have been given and the candidate is able to make informed and appropriate judgements within the context provided.</p> <p><i>There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</i></p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p>
			4-6 marks	<p>Candidate has described the impact of the loss of data for PH. Negative reasons have been described and the candidate is able to make some judgements within the context provided.</p> <p><i>There is a line of reasoning presented with some structure. The information presented is in the most-part relevant and supported by some evidence.</i></p> <p>Some subject specific terminology and knowledge will be used.</p>
			1-3 marks	<p>Candidate has identified points about the impact for PH.</p> <p><i>The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.</i></p> <p>At the bottom of the mark band the candidate may have simply provided a single point.</p>
			0 marks	Nothing worthy of credit.
Levels of response marking:				

Question		Answer	Marks	Guidance	
2	(a)	Three from, e.g.: <ul style="list-style-type: none"> Virtual attack (1) NOT environmental/physical (1) such as DoS (1) Where the attacker does not have to be physically present (1) using software to gain access (1) such as malware (1) 	3	Max 2 if no example. Allow mix and match Award example if virtual – e.g. delete data	
	(b)	Two from, e.g.: <ul style="list-style-type: none"> Show patterns of behaviour (1) if person is prominent individual other governments may be interested in whereabouts (1) Mapping data could be of a sensitive area (1) such as a military establishment (1) 	2		
3	(a)	(i)	One from, e.g.: <ul style="list-style-type: none"> Each individual knows what they have to do (1) There are clear task associated to each person (1) 	1	
		(ii)	One from, e.g.: <ul style="list-style-type: none"> To ensure everyone who needs to know is contacted (1) If not listed, might miss someone out (1) If there is panic, easier to follow a list than to try and remember (1) 	1	
		(iii)	One from, e.g.: <ul style="list-style-type: none"> Actions will not be forgotten (1) Some tasks require actions to be done in a specific order (1) Individual may not be familiar with procedures (1) Allows anyone to start the process (1) Gives a starting point / baseline (1) 	1	

Question		Answer	Marks	Guidance
	(iv)	<p>One from, e.g.:</p> <ul style="list-style-type: none"> To know which systems to focus attention on (1) To understand where to focus attention (1) Estimate time / cost required to fix (1) 	1	
(b)	(i)	<p>One mark for each correct statement in the correct position:</p> <p>THE CSIR needs to record the type of ATTACKER (1) so that they can understand their MOTIVATION (1). The CSIR will record the TECHNIQUES (1) used by the attacker.</p>	3	
	(ii)	<p>Three from, e.g.:</p> <ul style="list-style-type: none"> To see if there were common methods of attack (1) that can be predicted (1) and prevented (1) To understand if the same vulnerability is being used (1) across many systems (1) and specific to the company (1) To understand the cyber security landscape (1) and how other companies are being attacked (1) so preventative measures can be taken (1) 	3	
	(iii)	<p>Two from, e.g.:</p> <ul style="list-style-type: none"> There may have been no way to prevent the incident (1) Everything that could have been done was (1) The incident may have not been successful and the current procedures worked (1) The vulnerability might be a new one (1) and time is needed to analyse to come up with recommendation (1) 	2	<p>Do NOT accept “because it was missed out/not filled in”</p> <p>Do not accept don’t’ know what the vulnerability was...</p>

Question		Answer	Marks	Guidance
4	(a)	<p>One advantage, one disadvantage, two marks each, e.g.:</p> <p>Advantage:</p> <ul style="list-style-type: none"> • Can deter the criminal (1) from continuing (1) • Neighbours may investigate (1) minimising theft/damage (1) • Can alert Taylor (1) so they can call the police / take action (1) <p>Disadvantage:</p> <ul style="list-style-type: none"> • If repeatedly goes off (1) might be ignored (1) • People who hear it (1) might not know which house it belongs to (1) • Does not prevent (1) the attacked gaining access/not prevent (1) • Can be damaged/broken/hit (1) stopping it from making a sound (1) 	4	Disadvantage – allow responses related to not actually catching the criminal
	(b)	<p>Four from, e.g.:</p> <ul style="list-style-type: none"> • Fingerprint is scanned (and saved) (when lock is set up) (1) • Taylor's fingerprint is scanned (1) • Looked up in database to find match/compares with saved (1) • If match found, access granted (1) 	4	Not READS Not – does not unlock if no match

Question		Answer	Marks	Guidance
	(c)	<p>Three from, e.g.:</p> <ul style="list-style-type: none">• Monitor traffic against library/detect attack on the system (1) and notify Taylor (if an attack is detected) (1) allowing them to take remedial action (1)• Assesses the integrity of the system and data files (1) making sure that they have not been corrupted (1) or tampered with (1)• Identified errors system configuration (1) before an attack takes place (1) allowing Taylor to correct it (1)	3	

Question	Answer	Marks	Guidance								
5	Two from, 1 mark each, e.g.: <ul style="list-style-type: none"> • Theft/steal the phone (1) • Shoulder surfing (1) • Get user to install malicious app (1) • Smishing/Phishing(1) 	2									
6*	Indicative content may include: <ul style="list-style-type: none"> • Identify risks that may be present – weak/reused passwords. Signed up for websites with weak security, emails informing them that there has been a data breach of a website. Running old software. • Measure the risk – if the password has been compromised, how can it be used against them? What information and damage could be caused? • Monitor the risk - check accounts, logs, activity on the system. • Control the risk – how to mitigate the risk – changing passwords, running software version and automatic update tool, anti -virus software to be installed and updated. <p>A detailed focus on just ONE area is a max L2</p>	7	Levels of response marking: <table border="1" data-bbox="1366 523 2116 1241"> <tbody> <tr> <td data-bbox="1366 523 1473 794">5-7 marks</td> <td data-bbox="1473 523 2116 794">Candidate has explained how risk management should be used to protect digital vulnerabilities. The candidate is able to make informed and appropriate judgements within the context provided. Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</td> </tr> <tr> <td data-bbox="1366 794 1473 1002">3-4 marks</td> <td data-bbox="1473 794 2116 1002">Candidate has described how risk management should be used to protect digital vulnerabilities. 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 data-bbox="1366 1002 1473 1169">1-2 marks</td> <td data-bbox="1473 1002 2116 1169">Candidate has identified how risk management should be used to protect digital vulnerabilities. At the bottom of the mark band the candidate may have simply provided a single point.</td> </tr> <tr> <td data-bbox="1366 1169 1473 1241">0 marks</td> <td data-bbox="1473 1169 2116 1241">Nothing worthy of credit.</td> </tr> </tbody> </table>	5-7 marks	Candidate has explained how risk management should be used to protect digital vulnerabilities. The candidate is able to make informed and appropriate judgements within the context provided. Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.	3-4 marks	Candidate has described how risk management should be used to protect digital vulnerabilities. The candidate is able to make some judgements within the context provided. Some subject specific terminology and knowledge will be used.	1-2 marks	Candidate has identified how risk management should be used to protect digital vulnerabilities. At the bottom of the mark band the candidate may have simply provided a single point.	0 marks	Nothing worthy of credit.
5-7 marks	Candidate has explained how risk management should be used to protect digital vulnerabilities. The candidate is able to make informed and appropriate judgements within the context provided. Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.										
3-4 marks	Candidate has described how risk management should be used to protect digital vulnerabilities. The candidate is able to make some judgements within the context provided. Some subject specific terminology and knowledge will be used.										
1-2 marks	Candidate has identified how risk management should be used to protect digital vulnerabilities. At the bottom of the mark band the candidate may have simply provided a single point.										
0 marks	Nothing worthy of credit.										

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](https://twitter.com/ocrexams)

 [/ocrexams](https://twitter.com/ocrexams)

 [/company/ocr](https://www.linkedin.com/company/ocr)

 [/ocrexams](https://www.youtube.com/ocrexams)



CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT

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

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored. © OCR 2024 Oxford Cambridge and RSA Examinations is a Company Limited by Guarantee. Registered in England. Registered office The Triangle Building, Shaftesbury Road, Cambridge, CB2 8EA.

Registered company number 3484466. OCR is an exempt charity.

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.