

Cambridge Technicals IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT
05839 - 05842 & 05877

Mark Scheme for June 2023

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 2023

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 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.

Rubric Error Responses – Optional Questions

Where candidates have a choice of questions across a whole paper or a whole section and have provided more answers than required, then all responses are marked and the highest mark allowable within the rubric is given. Enter a mark for each question answered into RM assessor, which will select the highest mark from those awarded. (The underlying assumption is that the candidate has penalised themselves by attempting more questions than necessary in the time allowed.)

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 space
- Award Zero '0' if:
- anything is written in the answer space and is not worthy of credit (this includes text and symbols).
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.**
- 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)	One from, two marks: <ul style="list-style-type: none"> Economic data (1) how the economy is performing (1) future government investments (1) National security (1) troop movements (1) appointments/movements of key figures/PM/King (1) 	2	One mark for identification, second for expansion Can award expansion without identification For economic – allow financial, but expansion must not be personal Allow national secrets / military BOD classified data
		(ii)	One from: <ul style="list-style-type: none"> Economic data (1) National security (1) 	1	Do not award if the same as 1(a)(i) For economic allow financial / tax
	(b)		Two from e.g : <ul style="list-style-type: none"> Holds financial data/bank details of individuals (1) Stores personal/patient/employee details (1) Stores medical records of individuals (1) Data on new treatments can be stolen and sold on (1) They have weaker protection (than other organisations) (1) 	2	Allow sensitive Allow action from information e.g. to use the financial details to steal money NOT identity theft – if they say steal personal data to impersonate a patient – Award a mark for the personal data
2	(a)	(i)	Three from e.g. <ul style="list-style-type: none"> Cable locks (Kensington) (1) Safe (1) Alarm (1) Door lock (1) CCTV cameras (1) Guard dogs (1) Security guards (1) Biometric access (1) Keycards/swipecards/RFID (1) 	3	Must be physical

Question		Answer	Marks	Guidance								
	(ii)	<p>Two from, e.g.</p> <ul style="list-style-type: none"> • Encryption (1) • Passwords (1) • Access rights (1) • Firewall (1) • Anti virus/malware/spyware (1) • Backup (1) • Patch / Update management (1) • IPS (1) 	2	Must be software								
	(b)*	<p>Indicative content may include:</p> <ul style="list-style-type: none"> • The benefit may be the elimination of risk but the cost to the business may be that it goes out of business for example replacing all networks with standalone computers. • The cost of implementing a technical solution may still not prevent the data being hacked which means there is very little benefit for large cost • The human is the weakest link in any system and costs such as training may be wasted if the user does not follow through what they are supposed to do • May not be appropriate for the business, may lead to complex systems which will lose customers/clients • Likelihood of some of the recommendations being used to target the company is low. • Cost of introducing recommendation might be more than the asset is worth – if physical for example <p>Costs are NOT just financial: Time, complexity of systems, losing customers, losing donations.</p>	7	<p>Level of response marking:</p> <table border="1"> <tbody> <tr> <td>5-7 marks</td> <td> <p>Candidate has explained the costs and benefits and the link between them. The candidate is able to make informed and appropriate judgements within the context provided.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p> </td> </tr> <tr> <td>3-4 marks</td> <td> <p>Candidate has described the costs and benefits and the link between them. The candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p> </td> </tr> <tr> <td>1-2 marks</td> <td> <p>Candidate has identified costs and benefits.</p> <p>At the bottom of the mark band the candidate may have simply provided a single point.</p> </td> </tr> <tr> <td>0 marks</td> <td>Nothing worthy of credit.</td> </tr> </tbody> </table>	5-7 marks	<p>Candidate has explained the costs and benefits and the link between them. The candidate is able to make informed and appropriate judgements within the context provided.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p>	3-4 marks	<p>Candidate has described the costs and benefits and the link between them. The candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p>	1-2 marks	<p>Candidate has identified costs and benefits.</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.
5-7 marks	<p>Candidate has explained the costs and benefits and the link between them. The candidate is able to make informed and appropriate judgements within the context provided.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p>											
3-4 marks	<p>Candidate has described the costs and benefits and the link between them. The candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p>											
1-2 marks	<p>Candidate has identified costs and benefits.</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.											

Question	Answer	Marks	Guidance								
(c)*	<p>Indicative content may include:</p> <ul style="list-style-type: none"> • They may be charged under GDPR legislation if the recommendations were ignored and allowed a data breach • Employees may lose their jobs as the charity will receive bad publicity and no new donations • Volunteers may offer their services elsewhere as the charity does not take data protection seriously which leads to a lack of staff • Beneficiaries of the charity will suffer as they will not receive items/funding as the charity has fewer staff and or shut down 	10	<p>Level of response marking:</p> <table border="1" data-bbox="1120 312 2078 1369"> <tr> <td data-bbox="1120 312 1227 683">7-10 marks</td> <td data-bbox="1227 312 2078 683"> <p>Candidate has discussed the implications for stakeholders. Negative explanations have been given and the candidate is able to make informed and appropriate judgements within the context provided.</p> <p>There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p> </td> </tr> <tr> <td data-bbox="1120 683 1227 992">4-6 marks</td> <td data-bbox="1227 683 2078 992"> <p>Candidate has described the implications for stakeholders. Negative reasons have been described and the candidate is able to make some judgements within the context provided.</p> <p>There is a line of reasoning presented with some structure. The information presented is in the most-part relevant and supported by some evidence.</p> <p>Some subject specific terminology and knowledge will be used.</p> </td> </tr> <tr> <td data-bbox="1120 992 1227 1299">1-3 marks</td> <td data-bbox="1227 992 2078 1299"> <p>Candidate has identified points about the implications for stakeholders.</p> <p>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.</p> <p>At the bottom of the mark band the candidate may have simply provided a single point.</p> </td> </tr> <tr> <td data-bbox="1120 1299 1227 1369">0 marks</td> <td data-bbox="1227 1299 2078 1369">Nothing worthy of credit.</td> </tr> </table>	7-10 marks	<p>Candidate has discussed the implications for stakeholders. Negative explanations have been given and the candidate is able to make informed and appropriate judgements within the context provided.</p> <p>There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</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 implications for stakeholders. Negative reasons have been described and the candidate is able to make some judgements within the context provided.</p> <p>There is a line of reasoning presented with some structure. The information presented is in the most-part relevant and supported by some evidence.</p> <p>Some subject specific terminology and knowledge will be used.</p>	1-3 marks	<p>Candidate has identified points about the implications for stakeholders.</p> <p>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.</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.
7-10 marks	<p>Candidate has discussed the implications for stakeholders. Negative explanations have been given and the candidate is able to make informed and appropriate judgements within the context provided.</p> <p>There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</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 implications for stakeholders. Negative reasons have been described and the candidate is able to make some judgements within the context provided.</p> <p>There is a line of reasoning presented with some structure. The information presented is in the most-part relevant and supported by some evidence.</p> <p>Some subject specific terminology and knowledge will be used.</p>										
1-3 marks	<p>Candidate has identified points about the implications for stakeholders.</p> <p>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.</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.										

Question		Answer	Marks	Guidance
3	(a)	<p>Two from, e.g.:</p> <ul style="list-style-type: none"> Delete the malware/files with malware in them (1) Disable breached accounts/change passwords of breached accounts (1) 	2	<p>This is remove No marks for isolation</p> <p>Not total deletion / factory resetting / restore from backup</p>
	(b)	(i) <p>Two from e.g.</p> <ul style="list-style-type: none"> To identify how the attack occurred (1) and the method used (1) To put in appropriate measures (1) to remove the threat in the future (1) To identify the motivation of the attack(er) (1) e.g. an individual might be revenge (1) To identify a pattern (1) to prepare for future attacks (1) Link to real world activities (1) cyber attack may be part of a wider attack (1) Target will help understand the purpose (1) which can identify the attacker/motivation(1) To know where to invest (1) to add security to the right area of the system (1) 	2	<p>This is about the report. It is not about preventing a current attack</p> <p>Allow examples</p>

Question	Answer	Marks	Guidance
(ii)		3	If they have done 4 lines ignore the incident category which has two lines coming from it, – Max 2
(iii)	<p>Two from, two marks each e.g.</p> <ul style="list-style-type: none"> • The method of access used/type of attack (1) Physical / social engineering / coding (1) • Any scripting/coding involved (1) was it a well known script / specifically written (1) • Did it use a known vulnerability (1) purchased from a vulnerability broker (1) • Use a honeypot (1) and see how it is attacked (1) 	4	Not motivation/type of attacker

Question		Answer	Marks	Guidance
	(c)	Two from, e.g. <ul style="list-style-type: none"> • Key information (1) • Procedures (1) • Policies (1) • Controls (1) • Battle Book (1) 	2	Not cyber security incident report / Incident log This is not documentation completed whilst the attack is going on. Allow examples of documents
4	(a)	(i) <ul style="list-style-type: none"> • One from: <ul style="list-style-type: none"> • Only those that are allowed to have access can get to the files (1) • Restricting permission to authorised users (1) • Information is kept private/secure (1) 	1	Read whole response – do not award only accessible by person it is about / no one can access
		(ii) <ul style="list-style-type: none"> • Two from, e.g.: <ul style="list-style-type: none"> • Passwords (1) • Privacy screens (1) • Access rights (1) • Encryption (1) • Firewall (1) • IPS (1) • Locks (1) • 2FA (1) • Biometric (1) • Anti malware/anti virus (1) 	2	Must be a method physical or logical Not IDS

Question		Answer	Marks	Guidance								
	(b) (i)	One from: <ul style="list-style-type: none"> Assuring the accuracy of the data (1) Assuring the trustworthiness of the data (1) All modifications are authorised (1) 	1	Allow valid / correct / uptodate / reliable								
	(ii)	Two from, e.g. <ul style="list-style-type: none"> Validation (1) Verification (1) Permissions to edit (1) Log of changes (1) Send to end user for checking (1) Check data for accuracy/relevance (1) 	2	Must be a specific method – check on its own is TV Update is NE – update every month – NE, BUT check the data is accurate every month is a mark It must be HOW								
5	(a)	Two from: <ul style="list-style-type: none"> Financial gain (1) Espionage (1) Create havoc (1) 	2	Allow examples Not Thrill, Revenge, Publicity, righting perceived wrongs								
	(b)	One mark for each type of attacker: <table border="1" data-bbox="353 938 1144 1217"> <thead> <tr> <th>Cyber Security Incident</th> <th>Type of Attacker</th> </tr> </thead> <tbody> <tr> <td>Changing grades in a school</td> <td>Script kiddie (1)</td> </tr> <tr> <td>Employee releasing customer information to a rival firm</td> <td>Insider (1)</td> </tr> <tr> <td>Hacking a company and releasing information on salary gender imbalance</td> <td>Hactivist (1)</td> </tr> </tbody> </table>	Cyber Security Incident	Type of Attacker	Changing grades in a school	Script kiddie (1)	Employee releasing customer information to a rival firm	Insider (1)	Hacking a company and releasing information on salary gender imbalance	Hactivist (1)	3	CAO for type of attacker.
Cyber Security Incident	Type of Attacker											
Changing grades in a school	Script kiddie (1)											
Employee releasing customer information to a rival firm	Insider (1)											
Hacking a company and releasing information on salary gender imbalance	Hactivist (1)											

Question		Answer	Marks	Guidance
	(c)	<p>One from, three marks each, e.g.</p> <ul style="list-style-type: none"> Financial information (1) identity theft (1) could be used to set up fake direct debits (1) and steal money from the individual (1) Health information (1) individual might have an embarrassing condition (1) and be blackmailed to keep quiet (1) Online viewing habits (1) such as illegal pornography (1) could be blackmailed to prevent their release (1) 	3	<p>Allow mix and match, any order</p> <p>Look for a continuous theme related to a single use</p> <p>Read whole response – mark to candidates advantage</p>
6	(a)	<p>Three from:</p> <ul style="list-style-type: none"> Plain text turned into cypher text/scrambled data (1) Cypher text is meaningless / not understandable (1) Cypher text turned into plain text (1) Conversion done by algorithm / key (1) 	3	Do not allow unreadable or cannot be intercepted.
	(b)	<p>Three from, e.g.</p> <ul style="list-style-type: none"> No way round them/gaps in security (1) Prevent not deter (1) Forces the individual to be there in person (1) Can differentiate between authorised and unauthorised/allow access to those that are allowed only / limits access (1) Cannot be overloaded (1) 	3	This is NOT about methods

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)



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 2023 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.