Cambridge Technicals

IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT

05839 - 05842 & 05877

Mark Scheme for January 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.

© OCR 2025

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. 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.**

   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
		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)**		2 from, e.g: • Laptop (1) • Desktop (1) • Router (1) • Switch (1) • Server (1) • Printer (1) • Hardware (1) • Computer (1) • Software/by example (1) • Employees/Customers (1) • Data (1) • Information (1) • Documents / emails (1)	2	Allow named brands and types of software Customer data and Human data – award 1 mark Systems is TV
	(b)		4 from e.g: • Identify the data that the asset holds (1) how the data might be of use to an attacker/intentions of attacker (1) the impact (1) how it can be mitigated (1) • Identify the traffic that passes through the asset (1) whether it can be put together (1) into a usable stream of data (1) • Identify the systems that the asset has access to (1) what data they can get to in the linked system (1) and what access rights they have (1) • Look at what damage can be caused by the asset (1) allocate a category rating to the damage (1)	4	The question is how the risk can be analysed, do not accept answer to do with what the risk is. Allow mix and match of answers.

2	(a)	2 from, 2 marks each, e.g: • Will it reduce the amount of work that can be done? (1) time taken to look at and follow the policy (1) • Who is going to implement the policy (1) will it require additional staff (1) • When will it be implemented (1) how to make sure all staff/customers are aware (1) • Down time of the system to implement the change (1) loss of orders (1) • How to communicate the policy (1) so that all staff/customers are aware (1) • Training of staff (1) so they are aware of the new measure / how to use it (1) • Testing of the new security measure/control (1) to ensure new vulnerabilities have not been introduced (1) • Legal implications (1) does the new measure meet GDPR?(1) • Does it conflict with current work practices (1) can the staff still perform their normal actions (1) • Can measures be implemented into the existing system (1) is new equipment / software required? (1)	4	There are no marks for identifying security measures that could be introduced. Do not accept answers relating to cost

	(b)		2 from, 2 marks each, e.g: - Scans /analyses traffic/checks/inspects/detects/monitors (1) suspicious activity/anomalies (1) - Sends alarms/alerts/notifies/inform (1) so that a human can determine if the system is under attack (1) - Drops malicious packets (1) so the payload cannot be deployed (1) - Blocks traffic (1) so that data cannot be sent/received (1) - Produce reports/logs (1) showing areas of attacks/vulnerabilities (1) - Always on (1) can take action without human intervention (1)	4	Do not allow issues

	(c)		3 from e.g: • Only allows registered devices (1) to access files / log on (1) unknown devices cannot access resources (1) • Limit (1) where/when/who (1) they log on on from (1) • Can ensure software is up to date (1) by not allowing the device to connect (1) if it has a vulnerability (1) • Check installed software (1) and remove any with security issues (1) • Only allow specific software to be installed (1) that has been checked (1)	3	Allow mix and match. Do not allow preventing the machine being taken out of the workplace.
	(d)		3 from, e.g: • Other family members may use the device (1) and access files they are not supposed to (1) or install vulnerable software (1) • The connection uses the member of staff home connection (1) which might not be secure (1) and vulnerable to interception (1) // home is not as secure (1) as work (1) • Video conferencing meetings can be joined by unknown personnel (1) who can listen in on private business conversations (1) and gather data (1) • Don't know where the member of staff is connecting from (1) might be in a foreign country (1) and data intercepted (1) • If using own device (1) risk of virus / hacking (1) can gain access to company data (1) limited / cannot be managed (1) • More risk/threat on home networks (1) as not controlled/monitored (1) such as phishing emails (1) • Devices more likely to be stolen (1) as home may not have as good a security system (1) as the office (1) • Delay in company responding (1) to an incident (1) as off site (1)	3	Allow mix and match.

3	(a)		2 from, 2 marks each, e.g: • Inform the customers (1) what was taken (1) / so they can take action (1) • Notify authorities (1) as they might know who the criminal is (1) • Release a public statement (1) to prevent any blackmail/reduce reputational damage (1) • Disable accounts (1) so stolen information cannot be misused (1)	4	Do not allow any answers to do with encryption, blocking connection, backup – the data has already been taken.
	(b)		• Critical (1) • Minor (1) • Negligible (1) • Significant (1)	4	Any order, no substitution of words Ignore any description.

	(c)		2 from, 2 marks each, e.g:
			• ICO (1)
			   o Legal requirement (1)
			• Insurance company (1)
			   o So that the policy can be paid (1)
			• External specialist/cyber security specialist (1)
			   o Dedicated professional with more experience can assist in retrieving the situation (1)
			   o Can help find how the data was obtained / repair vulnerabilities (1)
			• Lawyers (1)
			   o To make sure all steps are followed / to mitigate legal liability (1)
				4	Not police, customers, suppliers, stakeholders or competitors
					If no organisation, then why cannot be awarded.
					
					For ICO – allow government / DPA

4			Indicative content may include: Transfer of viruses between networks One insecure network can be used to attack others especially is users reuse passwords across networks Core functions can be attacked bringing down multiple websites in DoS attacks causing lack of sales Location is not needed to hack into a network All countries need security and weakness in one can impact on them all. Legislation is different across different countries so what is illegal in one may be legal in another	7	Levels of response marking:	
					5 - 7 marks	Candidate has shown a detailed level of understanding by discussing the impact cyber security incidents can have as a global problem. 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.	
					3 – 4 marks	Candidate has shown a good level of understanding by describing the impact cyber security incidents can have as a global problem. 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.	
					1 – 2 marks	Candidate has identified point(s) relevant to the impact cyber security incidents can have as a global problem. 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.	
					0 marks	Nothing worthy of credit.	

5			Indicative content may include: Financial – bank account details can be taken and money stolen Identity theft – details to prove identity can be stolen and a fake identity set up Reputation – personal details can be released which damage the individuals reputation.	10	Levels of response marking:	
					7 - 10 marks	Candidate has shown a detailed level of understanding by explaining (more than one) why an individual needs to protect their personal data. Relevant examples will be used to support discussion and ideas will be expressed clearly and fluently.
					4 – 6 marks	Candidate has shown a good level of understanding by describing why an individual needs to protect their personal data. 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.
					1 – 3 marks	Candidate has identified point(s) relevant about why an individual needs to protect their personal data. 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.
					0 marks	Nothing worthy of credit.

6	(a)		2 from 2 marks each e.g: • Politician (1) to promote political agenda / social change (1) • Non vegetarian (1) to change their views (1) • Employee at a company that wastes energy (1) to try and save the planet (1) • Government (1) against its policies/political cause (1)	2	Allow any answer where the target is not for money but to try and change their mind Allow description without identification
	(b)		2 from 2 marks each, e.g. • Financial (1) not being paid enough money so claiming what they think they are owed (1) • Espionage (1) moving to a new firm and taking company secret with them (1) • Score settling/revenge (1) overlooked for promotion/if the company has "wronged" them (1) • Righting (perceived) wrong (1) correcting a mistake (1)	4	Allow alternatives to the identification is meaning is clear. Allow mix and match for motivation
	(c)		2 from, 2 marks each, e.g: • Phishing (1) clicking a link and giving up their password (1) • Social engineering/Insider (1) getting them to verbally give their details (1) • Shouldering (1) looking when they enter their password (1) • Clickjacking (1) targeting advertising than then loads different content (1) • Interception / eavesdropping (1) finding/reading emails/calls to gain personal data (1)	4	Must be specifically targeting a person – do not allow malware / virus on its own – needs to be targeting a person Reach the whole response.
	(d)		1 from: • Organisations/business/company (1) • Equipment / by example (1) • Information (1)	1	

			• Government (1)		

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**

in **/company/ocr**

▶ **/ocrexams**

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.