Cambridge Technicals

IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT

05839 - 05842 & 05877

Mark Scheme for June 2024

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 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).

   Team Leaders must confirm the correct use of the NR button with their markers before live marking commences and should check this when reviewing scripts.

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
BOD	Benefit of Doubt	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)**	**(i)**	• Information is accessible (1) • When required/at any time/on demand (1)	2	
		(ii)	2 from, e.g.: • Failover/redundant system (1) • Anti virus/anti malware (1) • Firewalls (1) • Cloud copy (1) • Backup (1)	1	Not general cyber security – it must specifically prevent non availability of data – e.g. anti virus can prevent ransomware, firewalls can prevent DoS
1	**(b)**		1 for identification, 2nd for description e.g: • Flood/broken pipes (1) ○ Water shorting the equipment (1) ○ Old pipes can break over time (1) • Earthquake (1) ○ Bricks falling on top of the equipment (1) • Fire/extension lead catching fire (1) ○ Equipment being incinerated (1) ○ Overloading plug sockets (1)	2	Read the whole answer and mark to candidates advantage. Threat can be in the description.
2	**(a)**		2 from: • Espionage (1) • Publicity /bragging/reputation (1) • Score settling /right perceived wrong /grudge (1) • Public Good (1) • Income generation / money /financial/blackmail (1) • Practice/gain experience (1) • Revenge (1)	2	DNA thrill as given in the question DNA Fun / Havoc

Question			Answer	Marks	Guidance
	(b)		2 from e.g: • Over emphasise abilities (1) • Use online scripts/do not write their own scripts (1) • Little or no hacking skills/experience (1)	2	
	(c)		2 from: • Hacktivist (1) • Cyber-criminal (1) • Cyber terrorist (1) • Scammer (1) • Phisher (1) • Insider (1) • Vulnerability Broker (1)	2	Do not allow Script Kiddie DNA Hacker (TV)
3	**(a)**	**(i)**	1 for type of incident, 1 for description: • Inaccessible/unavailable data (1) ○ Data in the file cannot be read (1) ○ Data not available to those with authorisation (1) ○ Deny access to data (1) • Modification of data (1) ○ Changing file permissions (1)	2	This is not about unable to access the account or the system but the individual files
		(ii)	1 for type of incident, 1 for description: • Information disclosure/doxxing (1) ○ Data passed to person/released without permission of the owner (1) • Theft (1) ○ Data taken from original location (1)	2	NOT identity theft

Question			Answer	Marks	Guidance
	(b)		2 from, 3 marks each, e.g: • Cannot open files (1) e.g. cannot send or receive emails (1) could lead to missing work deadlines (1) • Changing all passwords to new ones (1) have to come up with new passwords (1) find all websites and accounts and change them (1) • Distrustful of people (1) don't know who the hacker is (1) can restrict their integration into the community (1) • Identity could be cloned (1) bank accounts opened in new name (1) money taken (1)	6	Allow mix and match – must be a disruption to Charlie's life NOT financial, reputation or loss of privacy. Allow answers related to loss of files, job, personal safety, loss of trust (of others and of Charlie), increase in stress, emotional issues etc.
4	**(a)***		Indicative content may include: Loss of privacy: Loses control over who has access to the information. Causes stress and anxiety – does not known who knows what information about them. Financial: If credit card/bank account information is released this can have an impact on credit history, could lose the house and not be able to pay bills. Can lead to identity theft and take time to get new cards and accounts. Reputational damage: Difficulties in personal and professional relationships, people might not trust them with information and can lead to being ostracised from the neighbourhood.	7	**Mark band 3 (5 – 7 marks)** At the **top** of the band a thorough discussion which shows detailed understanding: • Explained how loss of privacy, financial and reputational damage have impacted on Charlie • Included relevant examples related to Charlie • *There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.* **Mark band 2 (3-4 marks)** At the **top** of the band an adequate discussion which shows sound understanding: • Described at least **one** impact on Charlie • Included some examples which may not be relevant and may at times detract from fluency of narrative. • *There is a line of reasoning presented with some structure. The information presented is*

Question			Answer	Marks	Guidance
					in the most part relevant and supported by some evidence. **Mark band (1-2 marks)** At the **top** of the level a **basic** justification, which shows **limited** understanding: • identification of generic points • limited use of subject terminology **0 marks** Nothing worthy of credit.
	(b)		2 for description e.g: Penetration Testing: • Checks for vulnerabilities in software/network/systems (1) • Find open ports / access into a system from outside/ scan system (1) • Allows for incorrect setup to be found (1) such as default router password (1) • Authorised attack on network/hire hacker (1) to test common vulnerabilities (1) Sandboxing: • Separate / virtual machine / isolated (1) with no connection to the network (1) • Suspected virus run in isolated area (1) where it will do no damage to the network (1)	4	
	(c)		2 from, e.g • Requires automated routines to test specific applications (1) which require specialist knowledge (1)	2	

Question			Answer	Marks	Guidance
			• Used in software development (1) rather than finished networks (1) • Charlie may not have the skills/equipment (1) to run it (1) • Charlie cannot do anything about it (1) if they find vulnerabilities (1)		
	(d)		6 from, e.g.: • Can hire a white hat hacker (1) to attack the system (1) and produce a report on vulnerabilities found (1) • Can run a software update report (1) to find all software that have updates available (1) and so vulnerable to broker (1) • Can run a free port scanner (1) to identify basic configuration errors (1) which would allow a hacker access (1) • Can improve password complexity (1) to make it harder for a hacker to guess (1) • Change password/username (1) on route away from default (1) • Update firmware / applications / run patches / updates (1) to remove security flaws/running latest version (1) • Can install more power sockets (1) to reduce risk of fire (1) • Can add blinds to the window (1) to prevent neighbour seeing screen (1) • Can move desk away from line of sight of neighbour (1) to prevent eavesdropping (1) • Can install anti virus/anti malware (1) to block incoming viruses (1)	6	Max 3 for identification of actions. Not switch computer off Not moving away from neighbourhood Do not allow encryption -this will not mitigate an attack. Allow anti spyware

Question			Answer	Marks	Guidance
			• Can install firewall (1) to compare traffic against rules and block (1) • Backup (1) so if files are deleted they can be retrieved (1)		
5	**(a)**		6 from, e.g: • Encrypted files can still be encrypted (1) making them inaccessible (1) • Not everyone will follow a procedure (1) cannot always enforce them (1) • Attacks on a system might not be related to procedures of cryptography (1) might be from a different area (1) e.g. insider (1) • Confidence might have led them to overlook areas (1) historical systems for example (1) • Insider knows procedures (1) and can by pass them (1) and has access to unencrypted files (1) or the key (1)	6	
	(b)		2 from, 2 marks each, e.g: • Pay the ransom (1) and get the decrypt key from the hackers (1) • Delete all files (1) and rebuild from the backup (1) • System reinstall (1) from scratch (1) • Hire a security company (1) who has the ability to decrypt the files (1) • Run anti virus/anti malware (1) to remove ransomware (1)	4	Must be related to removal of ransomware

Question			Answer	Marks	Guidance
	(c)*		Indicative content may include: For future planning of cyber security incidents – what data was targeted, how long it took to recover so they can put in pace a realistic plan if it was to happen again. To refine the existing plan – if anything is missing it can be included as a result of the incident meaning that a new plan is more comprehensive and has fewer gaps. To identify areas where the system currently has weaknesses – areas of the business that they were unaware might be affected, data that needs to be backed up that was not, or the method of backup being incorrect. Looking at how long it takes to rebuild a system and the impact of this – communication to customers, financial impact if no income during the rebuild time to how much reserves they would need for the company to survive.	10	**Mark band 3 (7 - 10 marks)** At the **top** of the level a thorough explanation which shows detailed understanding: • **Explained how CSIR** used by the company • Included relevant examples related to the business, data and recovery time are used to support discussion • *There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.* **Mark band 2 (4 – 6 marks)** At the **top** of the level an adequate explanation which shows sound understanding: • **Described how CSIR** is used**:** • Included some examples which may not be relevant and may at times detract from fluency of narrative. • *There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.* **Mark band 1 (1 – 3 marks)** At the **top** of the level a **basic** justification, which shows **limited** understanding: • identification of generic points • limited use of subject terminology **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

/ocrexams

/company/ocr

/ocrexams