Cambridge Technicals
IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT
05839 - 05842 & 05877

Mark Scheme for January 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.

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
BOD	Benefit of Doubt	MAX	Max
BP	Blank Page	NAQ	Not answered question
‸	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.

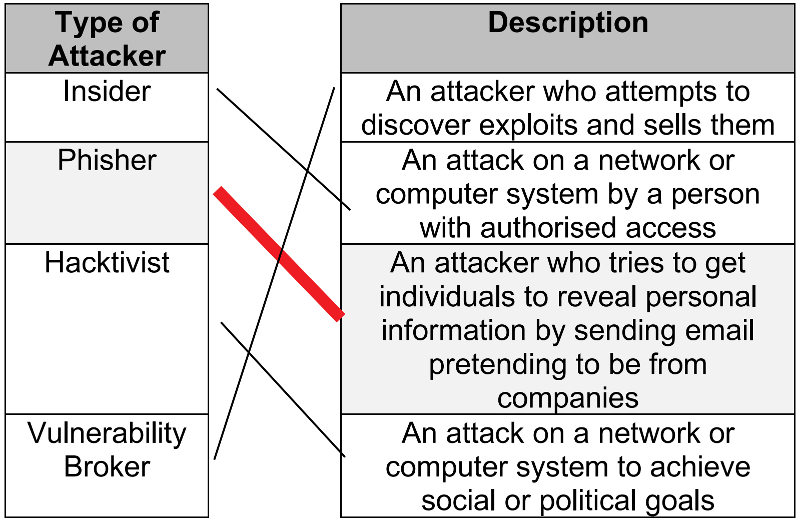
You should ensure that you have copies of these materials.

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)		Two from, one from each section, e.g.: • Data Modification: ○ Changing data (1) ○ Altering the contents (1) ○ Any other valid answer • Information Disclosure: ○ Data revealed/leaked (1) ○ Given to unauthorised people (1) ○ Sensitive information revealed (1) ○ Any other valid answer	2	MUST state which is which If they state CAN BE changed for example, this NE
	(b)	(i)	Two from, e.g: • Machine/data/system/network (1) is unavailable (1) • Services on the host (1) are disrupted (1) • Server crashes (1) and cannot fulfil requests (1) • Any other valid answer	2	NOT packets flooding the system
		(ii)	Two from, e.g.: • Increase bandwidth (1) • Blackholing/sinkholing (1) • Use of redundant network resources (1) • Limit number of requests (1) • Use of a firewall (1) • IPS (1) • Any other valid answer	2	NOT anti DoS software NOT IDS

Question			Answer	Marks	Guidance
		(iii)	One from: • Unauthorised access (1) • Inaccessible data (1) • Account lockout (1) • Hacking (1) • Escalation of privileges (1) • Destruction (1) • Malware (1) • Deliberate erasure (1) • Theft (1)	1	**NOT** DoS/DDoS, Modification, Disclosure **NOT** types of cyber criminal **NOT** social engineering **NOT** phishing / pharming Allow different types of malware
	(c)		Two from, two marks each. E.g.: • Righting perceived wrongs (1) finding information about runners who might have cheated (1) • Publicity (1) showing that the security for the club is not sufficient (1) • Fraud (1) To gain information about members to sell them fake running goods (1) • Income generation (1) to gain credit card details of members to steal money (1) • Identity theft (1) gaining Mia's personal data to impersonate her (1) • Any other valid answer	4	Second mark must be linked to Mia/Club What NOT how

Question			Answer	Marks	Guidance
	(d)		3 correct lines (3) 2 correct line (2) 1 correct line (1)  **Type of Attacker** Insider Phisher Hacktivist Vulnerability Broker **Description** An attacker who attempts to discover exploits and sells them An attack on a network or computer system by a person with authorised access An attacker who tries to get individuals to reveal personal information by sending email pretending to be from companies An attack on a network or computer system to achieve social or political goals	3	If two lines come from one type of attacker then mark as TV.
	(e)		Two from, e.g.: • Blackmail (1) might be health information that they don't want revealing to everyone (1) • Scam the members (1) by offering health solutions to their problems (1) • Any other valid answer	2	

Question			Answer	Marks	Guidance
	(f)*		Indicative content may include: • This will reduce the members confidence in Mia and might make them look for another club. • The website can be altered giving out false information which can make Mia look like she does not know what she is doing. • If the attacker uses a known vulnerability to gain access to the data then Mia could be responsible as she has not maintained the webserver. • Any other valid answer MUST be an impact on Mia	10	Level of response marking:

7 - 10 marks	Candidate has shown a detailed level of understanding by discussing the impacts on Mia of an attacker gaining access to the webserver. 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 explaining (at least one) the impact on Mia of an attacker gaining access to the webserver. 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 what an attacker can do if they were to gain access to the webserver. 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.

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th colspan="2">Guidance</th></tr>
<tr><td rowspan="5">2</td><td rowspan="5">(a)*</td><td rowspan="5"></td><td rowspan="5">Indicative content may include:

Positive
• If the data is intercepted it cannot be understood.
• Legal responsibility for security data.
• Gives confidence to the members that the protection of their data is being taken seriously.
• Any other valid answer

Negatives
• Only as strong as the weakest link, if weak encryption is used it may give a false sense of security.
• Encrypted files are more difficult to scan and there may be a virus that goes undetected.
• Encryption is only when the files are in transit, if someone gets hold of the device additional security measures are required.
• Any other valid answer</td><td rowspan="5">7</td><td colspan="2">Level of response marking:</td></tr>
<tr><td>5 - 7 marks</td><td>Candidate has evaluated the use of encryption. Both positive and negative benefits of the use of encryption 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 encryption. Positive OR negative benefits of encryption 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 encryption.

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

Question			Answer	Marks	Guidance
	(b)		Three from, e.g: • Devices allowed to access the data (1) are registered (1) • All other devices are denied access (1) • Each device (1) can only access specific data (1) • Authentication needs to be entered (1) before device can access data (1) • Allow valid example (1) • Any other valid answer	3	Note: this is the device NOT the individual
	(c)		Two from, two marks each, e.g: • Passwords (1) combination of letters/numbers/symbols only known to the user (1) • 2FA/Security questions (1) code sent to second device (1) • Firewall (1) set of rules to filter/block data (1) • Anti Virus / malware / spyware (1) files examined and if meet virus criteria they are deleted (1) • Patch management/Software updates (1) software vulnerabilities are removed (1) • VPN (1) hides information being sent/ received to webserver (1) • Any other valid answer	4	NOT encryption. NOT device management For firewall – NOT monitor traffic Must be software based (NOT physical) Allow IPS NOT IDS

Question			Answer	Marks	Guidance
3	(i)		One from: • Computer Misuse Act/CMA (1) • Data Protection Act /DPA (1) • Regulation of Investigatory Powers Act/RIPA (1) • Communications Act (1) • Copyright Designs and Patents Act (1)	1	Year is not required (ignore if incorrect) Allow GDPR
	(ii)		Three from, must all come from same act: Computer Misuse Act: • Applies to individual (1) • Need to make sure users known what is authorised (1) • No legal impact on organisation (1) Data Protection Act /DPA: • Appoint a DPO (1) • Make sure data is secure (1) through passwords/encryption (1) • Make sure data collected is used for its purpose (1) • Make sure data collected is not excessive (1) • Make sure data is accurate (1) • Not following it can result in a fine (1) Regulation of Investigatory Powers Act: • Cannot intercept (1) any communication without legal authority (1) • Only applies to public bodies (1) Communications Act: • Applies to individual (1) • No legal impact on organisation (1)	3	Must follow on from (i). If no answer is given in (i) but an act is given in (ii) then marks can be awarded. If no act is given in either, 0 marks can be awarded. Impact MUST be on organisation NOT individual Depending on the Act, may not be possible to achieve all marks

Question			Answer	Marks	Guidance
			Copyright designs and patents Act • Identify who owns the copyright (1) • Ask for permission (1) • Pay fee / credit owner (1)		
4	(i)		Two from, e.g.: • Can be cross referenced to other events (1) such as OS updates (1) • Can identify any internal actions (1) such as staff redundancy (1) • Allows logs to be examined (1) at the specific time of the attack (1) • Any other valid answer	2	This is NOT about identifying the incident but specifically why the date is needed Do not accept answers that are using the date as a method of filing
	(ii)		One mark per correct statement: • Significant (1) • Impact (1) • Critical (1) • Minor (1)	4	
	(iii)		Two marks for identification of group, two marks each for why the group needs to know e.g: • Police (1) ○ A crime has been committed (1) ○ To be able to investigate and prosecute (1) ○ Any other valid answer • Cybercrime units (1) ○ To identify methods used (1) ○ To assist companies with strategies for prevention (1) ○ Any other valid answer	6	These are people informed BEYOND those involved in the incident itself (NOT those in the who to contact section)

Question			Answer	Marks	Guidance
			• ICO (1) o Legal responsibility if personal data (1) o To create an overview of risk (1) o To understand the severity of the problem (1) o Any other valid answer • Customers (1) o To allow them to change passwords (1) o So they can be aware of any phishing attacks using the data (1) o Any other valid answer • Employees (1) o To know what precautions to take in future (1) o To be able to answer any external questions (1) o To know what personal precautions to take (1) if their own data was part of the incident (1) o Any other valid answer • Software manufacturers (1) o To know how the attacker got in (1) o To produce a path preventing it from happening again (1) o Any other valid answer		
5			Four from e.g: • Isolated environment (1) such as a standalone/virtual machine (1) • Not connected to network (1) so cannot spread (1) • Files can be opened/examined (1) • Any damage is limited to the one machine (1) • Any other valid answer	4	