Oxford Cambridge and RSA

Cambridge Technicals
IT

Unit 3: Cyber security

Level 3 Cambridge Technical in IT
05839 - 05842 & 05877

Mark Scheme for June 2022

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

TRADITIONAL

Before the Standardisation meeting you must mark at least 10 scripts from several centres. For this preliminary marking you should use **pencil** and follow the **mark scheme**. Bring these **marked scripts** to the meeting.

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 anyway 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 isn't an attempt at the question

   Note: Award 0 marks - for an attempt that earns no credit (including copying out the question).

8. 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.

9. Abbreviations, annotations and conventions used in the detailed Mark Scheme (to include abbreviations and subject-specific conventions).

Annotation	Meaning
/	alternative and acceptable answers for the same marking point
✓	Separates marking points
DO NOT ALLOW	Answers which are not worthy of credit
IGNORE	Statements which are irrelevant
ALLOW	Answers that can be accepted
( )	Words which are not essential to gain credit
__	Underlined words must be present in answer to score a mark

10. **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.

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>1</td><td>(a)</td><td></td><td>Indicative content may include:

• Legal requirements
o GDPR requires protection of personal data, if it is not then Nutz’N’Boltz may be fined
• Maintain customer base
o Reputation as a company that does not protect its customer data will likely make them go elsewhere/not get new customers in which will affect the profitability of the company
• Maintain employees
o If the employees data is not protected then they may not choose to work there and the company may have difficulty getting new staff affecting its profitability and ability to meet contracts
• Moral requirement
o Treat other peoples data how you want your own treated – do not allow access to it by anyone – easiest way to stop this is to protect it.
• Good business practice
o Gives the company a good reputation.</td><td>7</td><td>Level of response marking:

<table><tr><td>5-7 marks</td><td>Candidate has justified the need to protect personal information. Positive benefits have been explained and 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>3-4 marks</td><td>Candidate has described the need to protect personal information. Positive benefits 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 of protecting personal information.

At the bottom of the mark band the candidate may have simply provided a single point.</td></tr><tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr></table>
Positive answers only.
NOT method but WHY.</td></tr>
</table>

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td></td><td>(b)</td><td></td><td>One mark for identification, one for how targeted e.g.:
Server/Web Server (1)
• sql injection (1) getting them to run a webpage with code (1)
• xss/cross site scripting (1) malicious scripts executed by end user (1)

Router (1)
• Default passwords not updated (1)
• Firmware not updated that contains security exploit (1)

Laptop/Computer (1)
• Phishing attack to gain passwords (1)
• Keylogger/Malware installed (1)</td><td>4</td><td>If there is no identification of equipment anywhere in the answer, no marks can be given.

If equipment has been identified somewhere in the answer, marks can be awarded.

If the equipment identified and the method targeted do not match, then only one mark can be awarded for identification of equipment.

The methods for each item of equipment MUST be different.</td></tr>
<tr><td></td><td>(c)</td><td></td><td>Indicative content may include:

• Not all aspects can be tested
• Testing will only test known vulnerabilities
• Not 100% accurate – can give false sense of security
• Testing is limited to knowledge and understanding of the person doing the testing
• Changes may be made after testing that introduce vulnerabilities
• Testing will assist with staff training
• Testing will allow them to run through their responses and improve their response plan
• Will find any known issues/weaknesses and allow them to be corrected
• Will make sure all known software vulnerabilities are patched</td><td>10</td><td>Level of response marking:

<table><tr><td>7-10 marks</td><td>Candidate has evaluated the effectiveness of testing. Both positive and negative explanations have been given 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></table></td></tr>
</table>

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td></td><td></td><td></td><td>• Will allow company to get liability insurance</td><td></td><td>
<table>
<tr><td>4-6 marks</td><td>Candidate has described reasons for and against testing. Positive and negative reasons 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>1-3 marks</td><td>Candidate has identified points about the use of testing.

At the bottom of the mark band the candidate may have simply provided a single point.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table>
Positive AND negative required.
NOT monitoring
</td></tr>
</table>

Question			Answer	Marks	Guidance
2	(a)		Two from, two marks each, e.g.: • Allows people to go through a routine (1) the beginning of an incident can cause panic (1) • All those who need to be notified (1) will be (1) • Important first steps (1) will not be missed out (1) • Person on duty may not know the system (1) can follow a set of instructions (1) • Set of documented procedures may be tried and tested (1) to ensure that the problem can be resolved/does not spread (1) • They can be followed quickly (1) ensuring the incident does not spread (1) • Record of what was done is kept (1) showing that the individual/company made best efforts to tackle the incident (1) and can be used to fight any legal claims (1) • If a similar incident happens (1) they know how to act (1)	4	Max two for just identifications Max whole response to best advantage for candidate
	(b)		Two from, two marks each e.g.: • Disconnect from the internet (1) to prevent further access/data loss/restrict access (1) • Identify scope/type of incident (1) so all areas of infiltration can be examined (1) • Change passwords/disable accounts (1) in case they have been compromised (1)	4	
	(c)		Four from e.g.: • The hacker may have installed a back door (1) allowing them to return when NutZ'N'Boltz think the incident has passed (1)	4	

Question			Answer	Marks	Guidance
			• A keystroke/malware/trojan may have been installed (1) waits and causes problems in the future (1) • Passwords of customers may have been stolen (1) which has long term consequences (1)		
	(d)		Two from, two marks each, e.g.: • Employees (1) data released / may not feel safe / not enough employees to carry on (1) • Customers (1) data released and may not shop there again / loss of profits (1) • Infrastructure (1) contracts can be changed / leases altered and company not have any power / premises (1) • Equipment /wifi access point /Switch / Router (1) removing access to data (1) • Website/WebServer (1) if the website/webserver goes off line the company cannot sell any goods/make money and will go bankrupt (1) • Communication (1) messages cannot be sent to Africa and production will cease (1)	4	

Question			Answer	Marks	Guidance
3			Two from, two marks each e.g.: • Appoint a data protection officer (1) who is responsible for seeing that the law is met (1) • Only keep the data for as long as it is required (1) delete when no longer needed (1) • Check the accuracy of the data (1) regular audits of the data (1) • Only keep data that meets its purpose (1) data stored has a review date (1) • Allow access to the data subject on request (1) only their data can be passed on (1) • Data backup required (1) to be able to restore personal data (1)	4	One for identification, second for expansion/description GDPR principles (**excluding security)**

Question			Answer	Marks	Guidance
4	(a)		Data is accessible (1) When required (1)	2	
	(b)		Four from, CAO: • Biometric (1) • Swipe (1) • Updates (1) • Transit/Use (1)	4	
5	(a)		Three from: • Sent to undisclosed recipients (1) • Spelling error - Recipients /you(r) (1) • Hyper link is shortened / suspicious (1) • No personal information (customer/company) (1) • Poor grammar / Thanks you (1)	3	
	(b)		Three from e.g. • Never click a link in an email (1) always go direct to the site (1) • Search online to see if others have had the same email (1) • Install anti-phishing software/Send to Junk/Block (1) • Contact the sender to see if they have sent it (1) • Only open email if the sender is recognised (1)	3	Do not accept multiple marks for antivirus/malware/phishing software – award once only

Question			Answer	Marks	Guidance
6	(a)	(i)	Two from: • Conversion of plain text (1) • Into cypher/unintelligible/meaningless text (1) • Using key (1) • Method of storing/transmitting data so only the intended (1) can read it (1)	2	
		(ii)	Two from, e.g. • Symmetrical (1) • Asymmetrical / Public-Private Key (1) • Hash functions / MD5 / SHA-1 (1)	2	
	(b)		Three from, e.g • Deleting the file by mistake (1) • Not correctly removing pen drive (1) • Power surge (1) • Not powering computer off correctly (1) • Software crash/errors (1) • Hardware crash/errors (1) • Dropping the computer (1) • Misplacing/losing the device (1)	3	

OCR (Oxford Cambridge and RSA Examinations)
The Triangle Building
Shaftesbury Road
Cambridge
CB2 8EA

OCR Customer Contact Centre

Education and Learning
Telephone: 01223 553998
Facsimile: 01223 552627
Email: general.qualifications@ocr.org.uk

www.ocr.org.uk

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored

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 (Oxford Cambridge and RSA Examinations)
Head office
Telephone: 01223 552552
Facsimile: 01223 552553