OCR
Oxford Cambridge and RSA

Cambridge Technicals

IT

Unit 3**:** Cyber security

Level 3 Cambridge Technical Certificate/Diploma in IT
05838-05842, 05877

Mark Scheme for January 2018

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 will not enter into any discussion or correspondence in connection with this mark scheme.

Annotations

Annotation	**Meaning**
NAQ	Not answered question (answer given is for a different question)
MTP	Missed the point (has attempted the question, but has not dealt with the specific focus)
BOD	Benefit of the doubt (not right, but lingering doubt about whether it is correct)
NBOD	No BOD
TV	Too vague (answer does not include sufficient detail to be worthy of a mark)

Section A

Question			Answer	Marks	Guidance
1			TWO marks available, one e.g.: • Loss of customers (1) • Loss of sales(1) • Fine(1) • legal action (prosecuted under DPA)(1) • Loss of reputation (1)	2 (2xL)	Must be an impact on OCR phones and not to the customer. "**Customers lose faith/confidence**" type answers can be accepted. **"Customers will be forced to shop elsewhere"** type answers can NOT be accepted. Accept any awareness of legal action
2	**a**		Two marks available per explained answer. **Answer need not deal solely with security** **Security answer** • Breaking Data Protection Act (1) as the data has not been appropriately secured (1) • Hackers will be able to get into the system with ease (1) because holes in the software will be known (1) • If hacked, may be liable to pay individual damages (1) because it is the legal responsibility of OCR phones to update the software (1) **Non security answer** • Bugs in the software will not be fixed (1) and so customer service may be adversely affected (1) • Customer service impacted (1) resulting in customers going elsewhere (1)	6 (3xL) (3xH)	Only award two marks for an answer where there is an explanation of the implications. Answers should usually be in the form of identify implication (1) explain the implication (1)

Question			Answer	Marks	Guidance
2	b		Physical – identify TWO: Possible answers include • Security guards (1) • Biometric readers/access (accept eye scanners etc) (1) • Alarm systems (1) • Swipe cards(1) • Number pads (1) • Any other valid suggestion (1) Hardware identify TWO: Possible answers include • Safes (1) • Cable locks (1) • Any other valid suggestion (1)	4 (4xL)	Cameras do not improve security, they monitor. Do not allow repetition of answers across control types

Question			Answer	Marks	Guidance
2	c		MAX 4 marks for 2 full descriptions e.g. • Operational security policy (1) details what employees are allowed to do/escalation paths detailed/for example who to go to in OCR phones to un-filter a website (1) • Change management process (1) Process that defines how changes are made to the network/for example how upgrades are applied to OCR Phones servers – when and who does it (1) • Access control (1) Restrict access to devices that can connect to the network/for example not allowing personal phones to connect to the OCR Phones WiFi (1) • Authorization/access levels (1) Limiting the access of the employees to only that which is required, /for example not allowing employees access to personnel data (1) • Introduce firewalls (1) to control the flow of data into and out of the network (1)	4 (2xL) (2xM)	Identify operational security measure (1) plus example of that measure as applied (1) There is no need to identify OCR phone by name Accept any change to working procedure (day to day or longer term) (operational practice) to increase security of the network (by implication, this includes data on that network)

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>2</td><td>d*</td><td></td><td>Indicative content:

Accept any form of monitoring

e.g.

Employees
• Allows OCR phones to see what their employees are doing – are they following the correct procedures?
• Bad behaviour can be seen, such as leaving the account logged on which can lead to hacking.
• Can allow re training to occur based on what they employees are actually doing wrong.

Network/Firewall
• Can detect any traffic which is from a hacker and reduce the amount of damage that can be done.</td><td>10
(3xL)
(3xM)
(4xH)</td><td>Levels of response marking approach.

<table>
<tr><td>7 – 10 marks</td><td>Has shown a detailed level of understanding by discussing the use of monitoring as a method of reducing the likelihood of being hacked. The learner provides a clear discussion of more than one clear implication.

Relevant examples will be used to support discussion and ideas will be expressed clearly and fluently.

There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.</td></tr>
<tr><td>4 – 6 marks</td><td>Has shown a good level of understanding by explaining the use of monitoring by OCR Phones as a method of reducing the likelihood of being hacked. Explanations may concentrate on one implication, with, at the lower end of the mark band, limited depth.

Some examples used to support discussion may not be relevant and may at times detract from fluency of narrative.

There will be a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.</td></tr>
<tr><td>1 – 3 marks</td><td>Has identified points relevant to the use of monitoring to reduce the likelihood of being hacked. Limited use of examples to accompany description and ideas poorly expressed.

The information is basic and is communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit</td></tr>
</table>
</td></tr>
</table>

Question			Answer	Marks	Guidance
3	a		2 from, 2 marks each e.g. • Distributed Denial of Service (1) DOS attack from multiple computers (1) • Denial of service (1) flooding the server with requests so it cannot respond (1) • Malware/Virus (1) that deletes files preventing website being shown (1) • Keylogger (1) gain access to admin password and remove files (1) • Phishing (1) gain admin usernames and password by getting them entered into fake website (1)	4 (2xL) (1xM) (1xH)	
3	b		1 mark available e.g. • a cyber security incident that causes a loss of reputation/disruption of service/financial loss(1) • Where there is an impact to the running of one area of the business (1) • Where there is loss of data that needs to be reported (1)	1 (1xL)	Accept examples where relevant

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td>3</td><td>c</td><td></td><td>Indicative content:
• Will highlight areas of operational weakness in the organisations which can be addressed.
• Will show how the hack took place which allows OCR phones to patch the vulnerability.
• Highlights bad practices in OCR phones that can be exploited and allow future hacks to take place.
• Can be completed by external consultants who will see OCR phones with fresh eyes and not be used to exiting practices.</td><td>7
(2xL)
(2xL)
(3xH)</td><td>Level of response marking approach

<table><tr><td>5-7</td><td>Has shown a detailed level of understanding by explaining the importance of the report in preventing future incidents.

A conclusion may be given but may be implied.

Relevant examples will be used to support explanation</td></tr><tr><td>3-4</td><td>Has shown a good level of understanding by describing the importance of the report in preventing future incidents.

Some examples used to support description but may not be relevant</td></tr><tr><td>1-2</td><td>Has identified points relevant to the importance of the report.

Limited use of examples.</td></tr><tr><td>0</td><td>Nothing worthy of credit</td></tr></table></td></tr>
</table>

Section B

Question			Answer	Marks	Guidance
4	**a**		2 from, 2 marks each e.g. • (To) Protect personal data (1) which makes it less likely that your identity is stolen/your credit record destroyed which can prevent a mortgage in the future (1) • (To) Prevent unauthorised people accessing your home (1) connecter home with video/locks – criminals could steal physical items knowing when you are not there (1) • (To) Prevent theft of money (1) bank account could be emptied – when you try to pay at a restaurant there is no money so prevents embarrassment (1)	4 (2xL) (2xH)	Answers should be in the form of an identified reason (1) plus an explanation of that reason (1). Can be explained through the use of an example. Take "personal data" as meaning any data about the individual – this includes name etc, as well as bank details
4	**b**		1 from: Physical (1) Accept e.g. • Lack of receptionist on main door (1) • Lack of challenge to visitors/no identification of visitors (1) • No access controls on doors Environmental (1) • Natural disaster(1)	1 (1xL)	Not system attack. Allow examples of physical and environmental
4	**c**	**i**	Hacker who uses existing computer scripts (1)	1 (1xL)	Do not mark characteristics

Question			Answer	Marks	Guidance
4	c	ii	2 from, 2 marks each: e.g. • Lacks experience to write their own scripts/younger computer user (1) so relies on scripts written by others (1) • Unskilled in computer programming (1) searches and acquires scripts without understanding how they work (1) • Targets individuals with existing vulnerabilities (1) that they have scripts available to exploit (1) • Teenagers (1) who over emphasise their computing abilities (1) • Steals code (1) claiming it as their own (1)	4 (3xL) (1xM)	Must be a characteristic and not just an action
5	a		2 from, 2 marks each: e.g. • Identity theft (1) by stealing personal details (1) plus any impact of identity theft (1) • Financial/wealth (1) to gain bank details (1) plus any impact (1) • To steal intellectual property (1) to use for financial/reputational/commercial gain (1) • To target high profile targets (1) such as politicians (1) plus any impact (1)	4 (2xL) (2xM)	Identification is not required to gain the marks as long as the description has enough detail to know the type of motivation. Must be a motivation behind the attack. "To get data/information" is not enough.

Question			Answer	Marks	Guidance

5	b		First mark for identification of measure, second mark for how reduces risk
			
			e.g.
			• Use a password that you have not used before/different passwords for different accounts (or equivalent) (1)
			  ○ Only one account is affected if hacked (1)
			• Combination of character types/Use of numbers and symbols/Use of capitalisation (1)
			  ○ Dictionary attack cannot be used (1)
			• Increases the number of possible options (1)
			  ○ Correct password may be known but still not let the hacker in if the case is wrong – might think actual word is wrong and move onto to try a different one (1)
			• Do not use family member name/date of birth etc(1)
			  ○ Makes the password difficult to guess/password more random(1)
				4
				(2xL)
				(2xM)
					Only award answer to do with choosing a password. Do not award answers to do with maintaining security once the password has been chosen.
					
					Only award "password harder to figure out/guess/takes longer to work out password" as expansion <u>once</u>

6			1 mark for identified example, second mark for **matched** difference, repeat to max 4 overall e.g. Intentional • Deliberate actions (1) • Result of a harmful decision (1) • Planned set of actions designed to cause threat/damage (1) • Aware of the consequences of the actions (1) Examples e.g.: • Deliberate planting of computer virus (1) • Unauthorised use of username and password (1) • Social engineering (1) Accidental • Threat introduced without being aware of it (1) • Unintended consequence of an action (1)	4 (2xM) (2xH)	1 mark for example of intentional, one mark for example of accidental. 2 marks for differences can be obtained through a single contrasting statement Mark the whole answer The example must be an activity. Stating that the activity is to hack is not enough. **This must be a threat and not a consequence**

Question			Answer	Marks	Guidance
			• Not following policies (e.g. online store password policies) (1) Examples: • Leaving computer on when going for lunch (1) • Opening link on email (1)		

OCR (Oxford Cambridge and RSA Examinations)
1 Hills Road
Cambridge
CB1 2EU

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; 1 Hills Road, Cambridge, CB1 2EU
Registered Company Number: 3484466
OCR is an exempt Charity

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