Cambridge Technicals
IT

Unit 3: Cyber Security

Level 3 Cambridge Technical in IT

Mark Scheme for June 2019

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.

Annotations - Annotations available in RM Assessor

Annotation	Meaning
✓	Correct response
✗	Incorrect response
^	Omission mark
BOD	Benefit of doubt given
CON	Contradiction
RE	Rounding error
SF	Error in number of significant figures
ECF	Error carried forward
L1	Level 1
L2	Level 2
L3	Level 3
NBOD	Benefit of doubt not given
SEEN	Noted but no credit given
I	Ignore

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
ECF	Error carried forward
AW	Alternative wording
ORA	Or reverse argument

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.

Section A

Question			Answer	Marks	AO	Guidance
1	(a)		Two from, e.g. • To prevent (1) the same attack from happening again (1) • Identify target/motive/type (of attack) (1) to prevent/protect against it happening again (1) • To identify measures (1) to implement to protect the network (1) • To identify the scope (of the loss) (1) **plus expansion** (1) • To log/record/write down all information related to the incident (1) for (e.g) future reference (1) • To show vulnerabilities/weaknesses (1) so can be improved on (1)	[2]	4.1	**Do not accept:** • Any indication that attacks are monitored in real time **Further instruction** • Answers must be a description of the purpose – so look for an acceptable reason why the report will be written, answer should be in the form of **"what is done (1) and why this was done (1)"** • "To learn from the attack" – just enough for one mark (first answer) • Award any sensible expansion
1	(b)		10 marks, broken down as below **Title – one from**: **e**.g. • (Cyber) attack on/theft of Customer data (1) • (Cyber) attack on/theft of cyber-currency (1) **Target – one from**: e.g. • Customer data (1) • Private key (1) **Type of Incident(s) – one from** e.g. • Unauthorised access (1) • Theft/stealing funds (1) • Data breach/loss (1)	[10]	4.2	**Mark first answer given in any section (see comment re funds + in further instruction) other than techniques and impact sections ONLY, where mark first two (NB – only mark first two in impact section when candidate is identifying. Mark <u>first</u> description)** **Do not accept:** • Cyber security/attack/anything vague • Progressive Moniez/incident • Crypto currency as a target • Assets of the company as a target

Question	Answer	Marks	AO	Guidance
	Type of attacker(s) – one from e.g. • Cyber criminal (1) • Script kiddie (1) • Insider (1) • Organised crime (1) **Purpose of incident(s) – two marks for a full description (what done (1) and why (1))** e.g. • To acquire customer data (1) to sell to third party (1) • To gain private key (1) to steal money/financial gain (1) • To test a **known** vulnerability (1) to see if it works (1) and then repeat it against other companies (1) • To gain access to customer data (1) to access crypto currency (1) (**NB, If reversed and linked by "and" max 1 mark)** **Techniques used by attackers(s) – two marks for two techniques** e.g. • Identify/exploit vulnerability in **third party code/unpatched software** (1) • Attack the unencrypted NAS (1) • Use vulnerability broker/buy information off a vulnerability broker (1) • Use third party code (1) • Cryptography access methods (1) • Key logging (1) • Shoulder surfing (1) (**only accept when attacker is an insider)** • Social engineering (1)			• Transaction details as a target • Hacker/hacktivist as type of attacker • Phishing • "Employees not following security procedure" – TV (must state specifics for this answer) • Vulnerabilities in the system - TV **Further instruction** • NB, report produced internally, so no need to state "Progressive Moniez" for title. However, must be relatively unique and descriptive • Target must be a specific item, such as the private key, and not Progressive Moniez/customers/clients. ○ If answer in form of "funds" + customer data, ignore reference to funds • For description answers, answers may be taken from either part of the suggested answer for one mark, but only if answer makes sense (e.g. "financial gain" is ok, "to sell to a third party" is not). • Techniques may be two individual techniques identified OR one technique described • Techniques used by attackers MUST match the **type** of attacker

Question			Answer	Marks	AO	Guidance
			Impact on business – two marks for a full description OR explanation OR two individual impacts **Accept ANY reasonable impact on the business e.g.** • Loss of customer confidence/trust/reputation/respect (1) plus expansion (1) • Customer move to different company (1) plus expansion (1) • Bankruptcy (1) as have to pay loss to customers (1) • DPA/GDPR impact (1) plus expansion (1) • Get sued/civil legal action against you (1) • Taken offline (1) and so can not trade (1)			

Question			Answer	Marks	AO	Guidance
1	**(c)**		Up to six marks available. First mark for identification of target, **two** further marks for explanation: • Customers/Third parties (or examples of) (1st) ○ to access virtual wallets (1) by getting private key/to steal crypto currency (1) • Staff (1st) ○ Gain passwords (1) to access customer details database/NAS (1) ○ Because have a reputation for not following procedures (1) and so an easy target (1) • Equipment or example (1st) ○ Because machines are unpatched (1) and so old techniques can be used (1) ○ NAS is unencrypted (1) therefore is open access/an easy target (1) ○ (Employee phones) – could have stored **unencrypted** databases/information on their phones (1) which allows access to the Progressive Moniez network (1) • Data/Information (1st) ○ to be able to target customers (1) especially those who have reused passwords (1) ○ to acquire private key (1) and steal crypto currency (1)	[6]	2.4	**Do not accept** • Crypto currency • Key pairs **Further instruction** Candidate may repeat reason for attack and be awarded. Be aware of “such as” answers after a successful identification. These are **unlikely** to be an explanation of a reason. The reason for targeting any target MUST be linked to the overall scenario.

Question			Answer	Marks	AO	Guidance
1	(d)		Three from, two marks each, e.g.: • Signature based detection (1st) dictionary of patterns for each code exploit (1) • Sits behind firewall (1st) to provide an extra layer of security (1) (**Answer may be reversed**) • Examines/analyses network traffic flows (1st) to detect attacks (1) • Statistical anomaly detection (1st) samples network traffic and compares them to a baseline (1) • Sends alarm (1st) if anything abnormal/unauthorised access detected (1) • Alarm sent in real time (1st) so action can be taken immediately/whilst attack occuring (1) • Drops malicious packets (1st) to prevent access/infection (1) • Blocks traffic from source address (1st) to prevent entry (1) • Resets connection (1st) to remove active threat (1) (**Answer may be reversed**) • Works in (close to) real time (1st) as needs to protect against threats as they happen (1)	[6]	3.2	**Do not accept** • Firewall as part of the description of the IPS • Do not accept further features, such as must not negatively impact network speed • Host intrusion • IPS “takes action” - TV **Further instruction** First mark – identify feature Second mark – describe feature. **Do not award** if first mark not given The example answers may be mixed, so for example, accept: Scans for threats (BP3) to stop threat getting into the system (BP8)

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>AO</th><th>Guidance</th></tr>
<tr><td>1</td><td>(e)*</td><td></td><td>Indicative content:

Monitoring systems will only inform you of events after they have happened.

Will allow you to determine what happened and prevent it from happening in the future.

Need to act on the monitoring system, any delay could result in increased impact.

Monitoring systems may give false positives, so not have a system that reacts may mean honest users are not penalised.

Cost of the system needs to be weighed against the benefits – not a preventative measure.

Control systems restrict access to data/systems

Encryption/cryptography mean that any intercepted items can not be read without key.

Only as good as the level of security around them</td><td>[7]</td><td>3.1</td><td>Level of response marking:

<table>
<tr><td>5 - 7 marks</td><td>Candidate has evaluated the benefits of using monitoring AND control systems. Both positive and negative benefits of both systems 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.

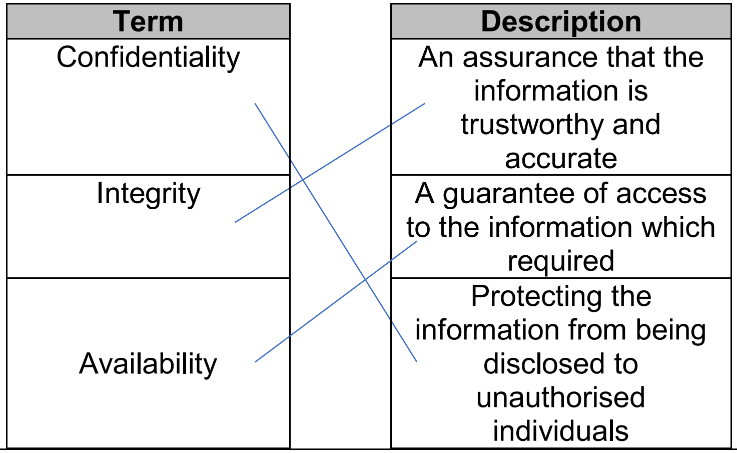
Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</td></tr>
<tr><td>3 – 4 marks</td><td>Candidate has described the benefits of using monitoring AND/OR control systems. Positive OR negative benefits of either system have been described 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 using monitoring AND/OR control systems.

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>
</td></tr>
</table>

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>AO</th><th>Guidance</th></tr>
<tr><td>2*</td><td></td><td></td><td><b>DO NOT accept identification of acts as worthy of marks</b>
<b>Implication MUST be on Progressive Moniez and NOT employees</b>
<b>GDPR/DPA</b><ul><li>Need to appoint data protection officer which will cost money.</li><li>Staff need to be training which takes time away from their job and costs money.</li><li>All customers need to be informed of the data that is held about the and how it is to be used. Consent needs to be obtained and recorded.</li><li>Customers can ask for details of all information that is held on them free of charge and if it is not all provided they can complain to the ICO.</li><li>A company that follows data protection guidelines is likely to have better security and gain more customers as customer confidence increases.</li><li>The data protection guidelines allow the company to ensure all aspects of data protection are covered rather than creating their own set of guidelines and policies.</li></ul><b>Computer Misuse Act</b><ul><li>Not allowed to timelock/disable software so no longer functions</li><li>Protected against malicious access to data by others (including employees) (where candidates describe or explain an impact on employees, this is likely to be sufficient for MB1, as has identified an implication)</li></ul></td><td>[10]</td><td>2.6</td><td>Level of response marking:<table>
<tr><td>7 - 10 marks</td><td>Candidate has shown a detailed level of understanding by discussing the impact of cyber security legislation.
Relevant examples will be used to support discussion and ideas will be expressed clearly and fluently.</td></tr>
<tr><td>4 – 6 marks</td><td>Candidate has shown a good level of understanding by explaining (at least one) the impact of cyber security legislation.
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) implication.</td></tr>
<tr><td>1 – 3 marks</td><td>Candidate has identified point(s) relevant about cyber security legislation.
Limited use of examples to accompany description and ideas will be poorly expressed.
At the bottom of the mark band, (a single) implication may be identified with an example.</td></tr>
<tr><td>0 marks</td><td>Nothing worthy of credit.</td></tr>
</table></td></tr>
</table>

Section B

Question			Answer	Marks	AO	Guidance
3	(a)		Max three, as below:  Term Confidentiality Integrity Availability Description An assurance that the information is trustworthy and accurate A guarantee of access to the information which required Protecting the information from being disclosed to unauthorised individuals	[3]	1.1	**Further instruction** If four lines used, max 2 If five lines used, max 1 If six lines used, no marks
3	(b)		Max three as below. One mark each: **Definition** Destruction (1) Modification (1) Inaccessible (1)	[3]	1.2	**Further instruction** • Allow alternate terms if the meaning is the same. • Do not accept a repeat of the question: ○ e.g "Locking access" for account locking
4	(a)		Four from, e.g. • Plaintext converted to encoded text/gibberish/scrambled/jumbled up(1) • By application of algorithm (1) • If **intercepted** cannot be understood (1) • Key/passcode used to convert back to plain text (1) • Without key/passcode cannot be read/understood//correct key needed to access data (1)	[4]	3.3	**Do not accept** • Unreadable • Formatted in code (TV)

Question			Answer	Marks	AO	Guidance
4	(b)		One mark available for any suitable method of protecting data e.g.: • Locking the memory stick in a safe (1) • Back up data (1) • Add a password to the files (1)	[1]	3.3	**Do not accept** • **Use** cloud or cloud based services (accept “back up to cloud”) **Further instruction** • Allow physical or logical security measures. • Ignore any reference to transferring to a different device (e.g. “cloud”) and consider method given

Question			Answer	Marks	AO	Guidance
5			Two from, two marks each: e.g. • Espionage (1st) obtaining information from competitors/governments (1) • Righting perceived wrongs/attacking named individual or organisation (1st) releasing information where an organisation has acted immorally/doing for the better of society/ (1) • Publicity/Pride (1st) highlighting their own skills (1) • Fraud (1st) using the information gained to result in personal/financial gain (1) • Score settling (1st) to get vengeance/retribution against person/organisation for something they have done to you (1) • Public good (1st) hacking to assist individuals/organisation (1) • Thrill (1st) hacking for excitement it brings when successful / fear of being caught (1) • Income generation (1st) stealing bank account details to acquire money (1) • Practice (1st) hacking to improve/maintain skills (1) • Sabotage//havoc and mayhem (1st) to cause damage (1)	[4]	2.3	**Do not accept**: • Answers based on a type of hacker – for example, “they are a hacktivist” • Personal gain (TV) • Money (TV) **Further instruction** • The motivation needs to be given before the description can be awarded. Accept equivalences for the motivations (score setting=spite and anger) • The descriptions are examples. • Read whole description and award to candidate’s best advantage • DO NOT mix and match

Question			Answer	Marks	AO	Guidance
6			Two from, two marks each, e.g.: • To test their security (1st) without running the risk of data being stolen (1) • Having their security compromised (1st) but no publicity to cause loss of customers (1) • To assist in building a computer system that is harder to hack (1st) by eliminated exploits hackers will use (1) (Answer may be reversed) • To create awareness of hacking in all areas of the company (1st) and get employees to follow the rules and procedures (1) (Answer may be reversed) • Ethical hacker will not exploit any issues that are found (1) and so is a safe person to check the network/and would want to help the organisation (1) • Ethical hacker would want to cause benefit (1) rather than harm (1)	[4]	2.6	**Further instruction** Answers in form of the reason (1st) plus a statement of why this reason is a reason (1).

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

Cambridge Assessment

LLOYD'S REGISTER QUALITY ASSURANCE ISO9001

UKAS MANAGEMENT SYSTEMS 001