Level 3 Technical Level
IT: CYBER SECURITY
J/507/6435

Unit 6 Network and cyber security administration

Mark scheme
January 2019

Version: 1.0 Final

Mark schemes are prepared by the Lead Assessment Writer and considered, together with the relevant questions, by a panel of subject teachers. This mark scheme includes any amendments made at the standardisation events which all associates participate in and is the scheme which was used by them in this examination. The standardisation process ensures that the mark scheme covers the students' responses to questions and that every associate understands and applies it in the same correct way. As preparation for standardisation each associate analyses a number of students' scripts. Alternative answers not already covered by the mark scheme are discussed and legislated for. If, after the standardisation process, associates encounter unusual answers which have not been raised they are required to refer these to the Lead Assessment Writer.

It must be stressed that a mark scheme is a working document, in many cases further developed and expanded on the basis of students' reactions to a particular paper. Assumptions about future mark schemes on the basis of one year's document should be avoided; whilst the guiding principles of assessment remain constant, details will change, depending on the content of a particular examination paper.

Further copies of this mark scheme are available from aqa.org.uk

Level of response marking instructions

Level of response mark schemes are broken down into levels, each of which has a descriptor. The descriptor for the level shows the average performance for the level. There are marks in each level.

Before you apply the mark scheme to a student's answer read through the answer and annotate it (as instructed) to show the qualities that are being looked for. You can then apply the mark scheme.

Step 1 Determine a level

Start at the lowest level of the mark scheme and use it as a ladder to see whether the answer meets the descriptor for that level. The descriptor for the level indicates the different qualities that might be seen in the student's answer for that level. If it meets the lowest level then go to the next one and decide if it meets this level, and so on, until you have a match between the level descriptor and the answer. With practice and familiarity you will find that for better answers you will be able to quickly skip through the lower levels of the mark scheme.

When assigning a level you should look at the overall quality of the answer and not look to pick holes in small and specific parts of the answer where the student has not performed quite as well as the rest. If the answer covers different aspects of different levels of the mark scheme you should use a best fit approach for defining the level and then use the variability of the response to help decide the mark within the level, ie if the response is predominantly level 3 with a small amount of level 4 material it would be placed in level 3 but be awarded a mark near the top of the level because of the level 4 content.

Step 2 Determine a mark

Once you have assigned a level you need to decide on the mark. The descriptors on how to allocate marks can help with this. The exemplar materials used during standardisation will help. There will be an answer in the standardising materials which will correspond with each level of the mark scheme. This answer will have been awarded a mark by the Lead Examiner. You can compare the student's answer with the example to determine if it is the same standard, better or worse than the example. You can then use this to allocate a mark for the answer based on the Lead Examiner's mark on the example.

You may well need to read back through the answer as you apply the mark scheme to clarify points and assure yourself that the level and the mark are appropriate.

Indicative content in the mark scheme is provided as a guide for examiners. It is not intended to be exhaustive and you must credit other valid points. Students do not have to cover all of the points mentioned in the Indicative content to reach the highest level of the mark scheme.

An answer which contains nothing of relevance to the question must be awarded no marks.

The following annotation is used in the mark scheme:

//	-	means alternative response
/	-	means an alternative word or sub-phrase
A.	-	means acceptable creditworthy answer
R	-	means reject answer as not creditworthy
NE	-	means not enough
I	-	means ignore
DPT	-	in some questions a specific error made by a candidate, if repeated, could result in the candidate failing to gain more than one mark. The DPT label indicates that this mistake should only result in a candidate failing to gain one mark on the first occasion that the error is made. Provided that the answer remains understandable, subsequent marks should be awarded as if the error was not being repeated.

Question	Guidance	Mark
1	**Mark is for AO1** Hacktivism promotes a political or social agenda. **R.** more than one box ticked	1
2	**Mark is for AO3** Cryptography. **R.** more than one box ticked	1
3	**Mark is for AO5** a key. **R.** more than one box ticked	1
4	**Mark is for AO2** Information security management. **R.** more than one box ticked	1
5	**Mark is for AO3** VPN users can be connected securely over the Internet. **R.** more than one box ticked	1

Question	Guidance	Mark
6	**2 marks for AO2** **1 mark** for example and **1 mark** for explanation, eg: • a password that would be more difficult to guess or crack, eg long, contains mix of case/symbols/numbers, not in dictionary/likely to be unique, ie not wife's name, birthday, single figure, etc	2
7	**2 marks for AO1** **1 mark** for definition, **1 mark** for expansion, eg: • the practice of sending emails // a type of social engineering pretending to be from reputable individuals or companies (**1 mark**) emails asking for information via websites linked from email (**1 mark**) to get them to reveal personal information such as passwords/credentials/bank details (**1 mark**) eg from bank leading to a fake login page which harvests credentials (**1 mark**).	2
8	**4 marks for AO5** **1 mark (max 4 marks)** for each action, eg: • employ strong passwords • logoff/disconnect/turn off Wi-Fi when no longer in use • avoid open or unencrypted public (wireless) networks // connect to trusted networks • use known/trusted hotspots/wireless networks • don't send sensitive data wirelessly – wait to be back in office, home, etc • use secure URLs / trusted websites, encrypted email, VPN, etc • use spyware etc / apply software updates/patches • encrypt data / stored data / external drives • turn off file sharing/airdrop options • change the name of device to something inconspicuous • disable JavaScript. **R.** similar actions, eg antivirus and antimalware.	4

Question	Guidance	Mark
9.1	**2 marks for AO5** **1 mark (max 2 marks)** for each example, eg: • retina/iris • voice recognition • face/facial • signature • gait. **R.** if more than two examples given, mark first two only.	**2**
9.2	**1 mark for AO5** **1 mark** for one advantage, eg: • hard to forge • no need to remember passwords • unique so **should be/in theory is** more/very secure. **R.** information used from stem, eg humans have unique characteristics // human features are unique (unless further justification given).	**1**
9.3	**1 mark for AO5** **1 mark** for one disadvantage, eg: • reliability of the system / hardware • setting up / maintenance costs • social acceptability • can be faked / pattern stolen / mismatch grants access • can't be changed if compromised, eg copied fingerprint • cosmetic/coloured contact lenses/other relevant factors which might distort result.	**1**

Question	Guidance	Mark
10	**4 marks for AO1** **Survey** **1 mark** for • identify entry points / vulnerabilities • gain information about targets. **Delivery** **1 mark** for • infiltration – able to get inside, modify code enabling entry, gain foothold • get an attack into position, eg get infected email distributed. **Breach** **1 mark** for • gain access (to system/data) by exploiting a vulnerability/using stolen credentials • bypass perimeter defences • privilege escalation. **Affect** **1 mark** for • carry out/complete attack, eg steal data, take down system • carry out and remove evidence / exfiltrate. **A.** other reasonable definitions that show the sequence of an attack, eg steal data (breach), exfiltrate (affect).	**4**

Question	Guidance	Mark
11.1	**2 marks for AO3** **1 mark (max 2 marks)** for each example, eg: • event log • user access log • audit log • (network) security log • firewall log • web proxy log • incident log • browsing history. **R.** if more than two examples given, mark first two only. **R.** network logs (from stem)	**2**
11.2	**2 marks for AO3** **1 mark (max 2 marks)** for each example, eg: • IP addresses • usernames of users accessing the network • time of log on and log off • location of user • software used • websites visited • files requested/accessed • tokens. Examiners should allow data from different types of access logs. **R.** if more than two examples given, mark first two only. **R.** passwords (unless a clear and credible explanation is given in 11.3)	**2**
11.3	**2 marks for AO3** **1 mark (max 2 marks)** for each point or expansion point, eg: • usage patterns in terms of time of day, day of week, and seasonally **(1 mark)** which can be used to look for unauthorised access **(1 mark)** • hardware use • printer, consumables use • monitoring staff use. **A.** use of valid alternative to answers from 11.2 **A.** password (attempts) if the explanation is credible	**2**

Question	Guidance	Mark
12.1	**2 marks for AO7** **1 mark (max 2 marks)** for each point, eg: • a password recovery tool (for Microsoft Windows) • decoding scrambled passwords, recovering wireless network keys, etc • recover/crack passwords, eg sniff network, capture passwords in transit, crack them • ethical recovery of passwords • stating methods of recovery, eg network packet sniffing, using lists/dictionaries.	**2**
12.2	**2 marks for AO7** **1 mark (max 2 marks)** for each point, eg: • cryptanalysis is the study of ciphers (**1 mark**) that is reading/analysing/deciphering encrypted code (without the key) (**1 mark**) • (In context) using rainbow tables to crack passwords (**1 mark**) which is plain text passwords and encrypted (pre-compiled/calculated) hashes (**1 mark**) • In this process tools match hashes with rainbow table (**1 mark**) • (the study of) analysing information systems (**1 mark**) in order to study the hidden aspects of the systems **(1 mark).**	**2**

Question	Guidance	Mark
13.1	**2 marks for AO6** **1 mark (max 2 marks)** for each point, eg: • disaster recovery service which provides all the equipment needed for the business to maintain service (**1 mark**) such as office space, furniture, telephone jacks and computer equipment (**1 mark**) • site already set up with hardware (**1 mark**) and copies of data (**1 mark**) • mission-critical site (**1 mark**) • back up/duplicate of the original site (**1 mark**) but a different site/location (**1 mark**) • site up and running continuously/real-time synchronization (**1 mark**).	**2**
13.2	**2 marks for AO6** **1 mark (max 2 marks)** for each point, eg: • disaster recovery service provides office space/power (**1 mark**), but the customer supplies the hardware (**1 mark**) • cold site is less costly as does not need hardware (**1 mark**).	**2**
13.3	**2 marks for AO6** **1 mark (max 2 marks)** for each point, eg: • disaster recovery service where hardware is pre-installed (**1 mark**) so that if disaster strikes, you can load your software and data to restore your connectivity (**1 mark)** • somewhere between hot/cold, some hardware (**1 mark**), data restored from backup (**1 mark**).	**2**

Question	Guidance	Mark
14	**4 marks for AO3** **1 mark (max 4 marks)** for each point, eg: • A honeypot is a computer system on the Internet that has been set up with intentional vulnerabilities / as a decoy (**1 mark**) which simulates the behaviour of the real system (**1 mark**) with which they're associated. It is used as a trap to attract hackers (**1 mark**) and to monitor/gather information about them and their methods (**1 mark**). Network administrators are alerted of the attempt (**1 mark**) and can get information about the attack. • A honeynet is two or more honeypots. (**1 mark**)	**4**

Question	Guidance	Mark
15.1	**4 marks for AO2** **1 mark (max 4 marks)** for each point of acceptable/unacceptable use, eg: • security around passwords and logins (except example given in stem) • limits of authorisation or specific business need to interrogate the system or data • not to connect / install any unauthorised device / software • not to store data on any unauthorised equipment • not to transfer data or software to any person or organisation outside without the written authority of the organisation • limits of higher authority with regard to IT systems and data • not to use for inappropriate/unlawful purposes, eg obscene material, hacking, interception of data, introduction of spyware, misuse of customer data etc • not to acquire material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation • not to bring the organisation into disrepute • intentionally wasting staff effort or other resources • corrupting, altering or destroying (or surreptitiously observing another user's password etc without their consent • denying access to the network and its services to other users • pursuance of unauthorised commercial activities • breach of industry good practice likely to damage the reputation of the organisation • consequences of breach • ethical exemptions from unacceptable use (eg academic freedom). **DNA.** examples given in stem of question, except with specific expansion. **R.** if more than four examples given, mark first four only. **R.** similar instructions	**4**
15.2	**1 mark for AO2** **1 mark** for: • Computer Misuse Act	**1**

Question	Guidance	Mark
16.1	**2 marks for AO4** **1 mark (max 2 marks)** for each point, eg: • the practice of testing a computer system, network or web application to find vulnerabilities (**1 mark**) that an attacker could exploit (**1 mark**) and reporting/advising client on appropriate changes (**1 mark**) • method for ethical hacker (**1 mark**) to exploit vulnerabilities in the system (**1 mark**).	**2**

Question	Guidance	Mark
16.2	**2 marks for AO4** **1 mark (max 2 marks)** for each point, eg: • a software application that monitors network or system traffic for malicious activities/unauthorised access (**1 mark**) • comes in many forms, eg host/network-based (**1 mark**) • identifying and reporting incidents, logging details / alerts user/network manager/administrator (to investigate) (**1 mark**).	**2**

<table>
<tr><th>Question</th><th>Guidance</th><th>Mark</th></tr>
<tr><td>17.1</td><td><b>6 marks for AO2</b>
Maximum 6 marks overall.
<b>1 mark (max. 3 marks)</b> for each guideline.
<b>1 mark (max. 4 marks)</b> for each relevant explanation/expansion as to how it will <b>prevent</b> a virus attack.
<b>Maximum 1 mark for each guideline/explanation pairing where either aspect (or the combination of) is not clear.</b>
<b>Indicative content, eg:</b>
Risks from unknown senders, links, files/attachments, machines without antivirus software/or not updated/regularly checked, individual behaviour/practices.
Explains need to delete / not open unknown content, to avoid use of USB keys or scan before use, to avoid unauthorised software / use of unauthorised hardware, install antivirus on all endpoints, need for updating, configuring correctly, exclusions to antivirus checking/authorisation, analysis of antivirus logs, managing risk.</td><td>6</td></tr>
<tr><td>17.2</td><td><b>9 marks for AO2</b>
Mark using the levels of response table.
<table>
<tr><th>Level 1
1-3 marks</th><th>Level 2
4-6 marks</th><th>Level 3
7-9 marks</th></tr>
<tr><td>Awareness of symptoms, eg systems running slow, apps not working correctly / fully, PC stops / locks.</td><td>Reference to specific examples, eg printing failure, error messages, dialogue boxes / menus not responding / distorted, folders hidden / cannot be accessed, unusual emails.</td><td>Develops explanation to include, eg
• impact on business, working time lost
• cost of repair / recovery
• loss of customer confidence
• loss of data
• breach of DPA.</td></tr>
<tr><td>Makes reference to threat to business (loss of data, loss of function) and / or source of virus (USB stick, email, Internet).</td><td>Understands role of virus in, eg remote access, diverting private data, deleting files / stealing information, corrupting software / making PC unusable, copying key log information, eg passwords, credit card details, usernames.</td><td>Develops explanation to include, eg
• role of specific types of virus and potential damage
• loss of reputation
• reasons for policies
• topical discussion, eg NHS WannaCry attack, Equifax mass data breach, Stuxnet</td></tr>
</table>
</td><td>9</td></tr>
</table>

Question	Guidance	Mark
18	**15 marks for AO7**	15

Mark using the levels of response table. No marks are given for the format or level of formality in the answer other than the criteria below (understands, develops etc).

Level 1 **1-5 marks**	**Level 2** **6-10 marks**	**Level 3** **11-15 marks**
Awareness of management's view of risk, sets out some procedures	Identifies specific procedures, eg individual responsibilities, plans, hardware and data.	Develops explanation to include clear procedures, mostly in context, which include 'loss of data'.
Is aware of risks from visitors, contractors, home workers.	Understands need / dependence upon individual responsibility for confidentiality and adherence to policy and procedures.	Develops explanation to include (consequences of not adhering to) plan (business interruption, loss of business, crisis), ways of protecting data (eg encrypted files).
Makes reference to backup and storage, frequency, key data.	Understands role, value, and use of specific types of storage and media.	Develops explanation to type of backup and how named use of storage / media could be most effective in ensuring rapid recovery of IT content / business continuity.

Example:

This document details data handling procedures for home workers. These procedures must be followed to ensure the safety of company and personal data. It also covers the steps that must be followed in the event of an incident.

- Access to company systems is limited to company issued devices. Such devices are encrypted to protect data.
- Corporate data must be saved on the network server and not be stored locally on company laptops or home equipment. Loss of data may occur if it is stored in other locations, where it is not backed up or exposed to visitors and contractors.
- Backups will be carried out periodically in accordance with company policy. Employees must not backup data to local media which may prevent efficient recovery of data. Exposure/theft of data may occur if it is stored outside of protected company locations.
- In the event of loss/theft of company equipment or data the situation must be reported to IT immediately at any time of day or night and it is the responsibility of the employee to know whom to contact.

Question	**Assessment Outcomes**								**TOTAL**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	
SECTION A									
1	1b (1)								1
2			3d (1)						1
3					5b (1)				1
4		2b (1)							1
5			3e (1)						1
6		2a (2)							2
7	1a (2)								2
8					5b (4)				4
9.1					5b (2)				2
9.2					5b (1)				1
9.3					5b (1)				1
10	1c (4)								4
11.1			3f (2)						2
11.2			3f (2)						2
11.3			3f (2)						2
12.1							7d (2)		2
12.2							7d (2)		2
13.1						6b (2)			2
13.2						6b (2)			2
13.3						6b (2)			2
14			3f (4)						4
15.1		2c (4)							4
15.2		2b (1)							1
16.1				4b (2)					2
16.2				4b (2)					2
Total A	**7**	**8**	**12**	**4**	**9**	**6**	**4**	**0**	**50**
SECTION B									
17.1		2c (6)							6
17.2		2a (9)							9
18							6abc (15)		15
Total B		**15**					**15**		**30**
Total A+B	**7**	**23**	**12**	**4**	**9**	**6**	**19**	**0**	**80**