LEVEL 3 TECHNICAL LEVEL
IT: Cyber Security

J/507/6435 - Unit 6 Network and Cyber Security Administration
Mark scheme

June 2018

Version/Stage: 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.

Question	Guidance	Mark
01	C	1
02	B	1
03	D	1
04	C	1
05	C	1

Question	Guidance	Mark
06.1	**State two ways of preventing loss of data when there is a power cut.** **1 mark** (max 2 marks) for each way, eg: • uninterruptible power supply/source (UPS) • specific types of UPS, eg kinetic energy (flywheel), compressed air • alternate battery technologies • laptop battery • back-up generator • redundant power supply • continuous backup eg via operating system or program/app • mirroring, shadow disk etc.	**2**
06.2	**Cloud storage and DVD are two methods of backing up data.** **State one disadvantage of each method.** **1 mark** (max 2 marks) for each disadvantage, eg: Cloud storage: • cost • upload/download time, bandwidth, etc • potential issues of trust/security • access to internet required • internet link likely to be slower than local backup. DVD: • technology becoming obsolete • limited capacity of disk • security, eg easily stolen, drive used to steal other data • can't always be rewritten • more expensive/time consuming than magnetic media.	**2**
		Total 4 Marks

Question	Guidance	Mark
07.1	**What type of data was covered by the Data Protection Act?** **1 mark** (max 1 mark) for a type, eg: • personal data • data **stored on a computer** • data stored on an organised **paper filing system** • data about **living people**.	**1**
07.2	**State one principle of the Data Protection Act.** **1 mark** (max 1 mark) for one principle, ie: **Personal data** shall: o be processed fairly and lawfully o be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose o be adequate, relevant and not excessive o be accurate/kept up to date o not be kept for longer than is necessary o be processed in accordance with the rights of data subjects under this Act o not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection. o Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	**1**
07.3	**On May 2018, the General Data Protection Regulation (GDPR) replaced the Data Protection Act.** **State two ways the need for consent underpins the GDPR.** **1 mark** (max 2 marks) for each way, eg: • individual right to erasures • privacy impact assessment • personal data now includes online identifiers, location data, and genetic data • parental consent for minors required • individuals must opt-in • must be clear privacy notices • consent must be able to be withdrawn at any time.	**2**
		Total 4 Marks

Question	Guidance	Mark
08	**Explain how an office cleaner could help to mount a cyber attack on a company.** **1 mark** for each point or expansion point (max 4 marks), eg: • exploiting trust, eg by appearing authentic, theft of data/information, bribes • fake ID or credentials left lying around • could attach physical devices such as keylogger • specific examples, eg secretly observing/recording password entry, access to cables while office closed (documents, passwords left written down/in bins, installing devices which tunnel out).	**4**
		Total 4 Marks

09.1	**Describe a situation where encryption might be a problem.** **1 mark** for situation, **1 mark** for expansion point, eg: • preventing terrorism/law enforcement, intelligence services unable to decrypt intercepted data • forgotten password/lost or corrupted keys, prevents legitimate retrieval of data • cyber attack, attackers can use encryption to hide malware and launch attacks • testing / pen test that requires access to data.	**2**

09.2	**Some politicians have talked about banning encryption.**
	
	Explain what problems this might cause.
	
	1 mark (max 4 marks) for each point or expansion point, eg
	• the need for confidentiality, eg commercial
	• the need for security, eg online banking/fraud
	• the need to communicate securely, eg within oppressive state
	• state could spy on communications between citizens – lack of privacy/human rights issues
	• the consequences of interception/visibility of unencrypted information, eg helps criminal gangs
	• real-world examples (expansion points must be different), eg
	  ○ online banking uses encryption to log on/exchange information (**1 mark**) and without encryption their identity is at risk of being stolen (**1 mark**)
	  ○ exchanges between a lawyer and a client are confidential (**1 mark**) and without encryption this could be leaked online/to the media (**1 mark**).
		4

		Total 6 Marks

Question	Guidance	Mark
10.1	**Describe what is meant by an 'agitation campaign'.** **1 mark** (max 3 marks) for each point or expansion, eg: • a campaign to achieve political objectives/mobilisation/social change • to present a single idea to the masses, rouse emotions • origins in Russia, other restricted countries, but effect now international.	**2**
10.2	**How might an agitation campaign work on Twitter or Facebook?** **1 mark** (max 1 mark) for a point, eg: • create false/distorted/partisan narrative **(1 mark)**, eg links to articles, perhaps fake/bot-driven **(1 mark)** • tweets with hashtag sent to figures with large number of followers • tweets with links to information via URL • potential example, eg possible interference in US election, UK referendum.	**1**
		Total 3 Marks

11	**In the USA, TEMPEST was a National Security Agency programme that involved the monitoring (and shielding) of devices that unintentionally emit signals called 'leaking emanations'.** **Give two examples of 'leaking emanations'.** **1 mark** (max 2 marks) for each example, eg: • electromagnetic radiation from a monitor (**1 mark**) or a keyboard (**1 mark**) • radio or electrical signals • sounds • vibrations eg through walls, pipes • from cables, phone lines, conduction/crosstalk (**1 mark**) because they are poorly grounded (**1 mark**).	**2**
		Total 2 Marks

Question	Guidance	Mark
12.1	**Explain what is meant by the 'scope' of a penetration test.** **1 mark** (max 4 marks) for each point or expansion point, eg: • what is to be tested/included/excluded (**1 mark**) eg website to be tested / paths within site (**1 mark**) • agree which domains, IP addresses etc to test (**1 mark**) + expansion (**1 mark**) • agree what types of test to perform (**1 mark**) eg white box, black box (**1 mark**) • agree external perimeter (**1 mark**) and critical systems (**1 mark**) definitions • agree when to test, eg hours, dates/test period (**1 mark**) • agree lines of communication (**1 mark**) eg secure methods of communication, final report (**1 mark**) • obtain permission to speak to third parties **(1 mark**) eg hosting companies, service suppliers etc (**1 mark**) • agree timeline, eg Gantt chart (**1 mark**) • focus areas, eg check access controls effective (**1 mark**) Candidates must cover at least two bullets for 4 marks.	**4**
12.2	**Describe two ways a penetration test is different from a vulnerability scan.** **1 mark** (max 2 marks) for each difference, **1 mark** (max 2 marks) for each expansion point, eg: • exploit/circumvent/defeat rather than identify, rank, report. • penetration test usually less frequent, usually an interim process of identifying/fixing vulnerabilities • penetration test may have more manual input/take more time over automated (vulnerability) processes • penetration test may last days or weeks or grow in complexity, vulnerability scan relatively short/more fragmented.	**4**
		Total 8 Marks

Question	Guidance	Mark
13.1	**Explain, giving examples, the difference between 'authentication' and 'access control'.** **1 mark** (max 2 marks) for each explanation, **1 mark** (max 2 marks) for each example, eg: Authentication: • The process of verifying a user is who they claim to be, eg username and password, smart card, PIN, Apple Pay • An application trying to use a web services API. Access control: • Restricting access based on something other than the identity of the user/application, eg access to files based on user-type (administrator, etc), host name/address of machine requesting document, physical location, security clearance.	**4**

13.2	**Describe two examples of access control security models.**
	
	1 mark (max 2 marks) for each example, **1 mark** (max 2 marks) for expansion point eg:
	• Mandatory Access Control (MAC):
	  ○ constrains the way a subject performs operations on an object (files, directories, ports, etc) eg dependent on their level of trust/security clearance, and/or classification of file
	  ○ access set/controlled by an administrator.
	• Discretionary Access Control (DAC):
	  ○ based on the identity of subject or groups to which they belong
	  ○ control in the hands of an individual.
	• Role-Based Access Control (RBAC):
	  ○ restricting system access to authorised users acquired through role (esp. large organisations), eg civil service, based on need
		4

		Total 8 Marks

Question	Guidance	Mark
14.1	**Describe the CHECK assurance scheme.** **1 mark** (max 2 marks) for each point, eg: • NCSC involvement • penetration test • (government) approved companies • qualified personnel, eg CREST.	**2**
14.2	**Name two types of organisation that use the CHECK assurance scheme.** **1 mark** (max 2 marks) for each organisation, ie: • Her Majesty's Government • Other public-sector bodies.	**2**
14.3	**List two principles of CHECK membership.** The following principles form the basis of the CHECK service. **1 mark** (max 2 marks) for each principle, ie: • All CHECK companies must be able to sign-up to English law. • Any company accepted into CHECK must have performed penetration testing for a minimum of 12 months. • If an application to join CHECK is rejected it cannot be resubmitted within a 12-month period. • All team members must be able to obtain and hold an SC clearance. • The NCSC will sponsor an SC clearance, if required. • To be accepted as a CHECK Team Member each individual will have passed one of the CHECK Team Member examinations and must provide a personal CV. CHECK Team Leaders…. will have at least 12 months penetration testing experience. • If a member of a CHECK team transfers, it is the responsibility of the importing CHECK company to verify the status of the individual's clearance. • Membership is valid for a period of 1 year at a time. • In order to undertake work under the terms and conditions of CHECK, a Company must hold 'Green Light' status, which is achieved by at least one individual of the CHECK team holding CHECK Team Leader status.	**2**
		Total 6 Marks

Question	Guidance	Mark
15.1	**Name the three components of a TCB.** **1 mark** (max 3 marks) for each component, ie: • hardware • firmware • software.	**3**
15.2	**Explain how the design and implementation of a system's TCB affects its overall security.** **1 mark** (max 3 marks) for each point, eg: • bugs or vulnerabilities inside the TCB could compromise the security properties of the whole system • important to not leak privileges outside the TCB, eg components outside of the TCB need to not be able to leak data obtained from the inside • size of TCB important, eg so code base can be feasibly examined, as small as possible to make it practical to review security • software portions need to protect themselves from tampering; supervisor mode • hardware: CPU memory management unit, allow and deny access to specific ranges of the system memory to the programs being run; TCB in ROM.	**3**

<table>
<tr><th>Question</th><th>Guidance</th><th>Mark</th></tr>
<tr><td>15.3</td><td>
The WannaCry ransomware attack in May 2017 targeted computers running the Windows operating system, including many in the NHS in England.

Discuss reasons why the NHS computer network might have been vulnerable to an attack.

Candidates may explain “technical” element using either AO1 (eg objectives/stages) or AO2-AO5 (eg strategic, tactical, operational). Specific knowledge of either the NHS or WannaCry is not required.

Mark using the indicative content and the levels of response grid below:

Indicative content:
• technical and risk management issues
• network policies, eg an assessment of 88/236 trusts by NHS Digital before the attack found that none passed the required cyber-security standards[1]
• lack of central compliance monitoring by Department of Health
• most running Windows XP, which was no longer supported, or Windows 7
• operating system not security-patched
• lack of staff awareness/training (staff more likely to act on infected emails), also complacency (‘no one would attack a hospital’)
• alerts previously issued to trusts not acted upon (and not obliged to do so)
• firewalls not well managed at local level
• failure to upgrade old computer systems, eg those not capable of running Windows 10 (which had not been deployed/was not affected)
• lack of funding, eg money diverted to other areas/not ring-fenced.

<table>
<tr><th>Level</th><th>Descriptor</th><th>Marks</th></tr>
<tr><td>3</td><td>Clear contextual understanding of technical and risk management issues, which are explained holistically towards the top of the band.</td><td>7-9</td></tr>
<tr><td>2</td><td>Some understanding of technical and risk management issues, with some clear, contextual explanations towards the top of the band.</td><td>4-6</td></tr>
<tr><td>1</td><td>Lists some technical or risk management issues, or some fundamentals of cyber attacks.</td><td>1-3</td></tr>
<tr><td></td><td>No creditworthy response</td><td>0</td></tr>
</table>
</td><td>9</td></tr>
<tr><td colspan="3">Total 15 Marks</td></tr>
</table>

[1] http://www.bbc.co.uk/news/technology-41753022

Question	Guidance	Mark
16.1	**Name three other locations in a computer system where data could be hidden.** **1 mark** (max 3 marks) for each location, eg: • directory not immediately visible to user (eg system) • memory • slack space • hidden directories • in blocks/bad blocks • alternate data streams (or transmission of data) • hidden partitions • specific amplification of 'file within a file', eg virus/data/virus/data/another image within an image.	**3**

Question	Guidance	Mark

16.2	**Explain methods that computer forensic analysts use to collect and preserve digital evidence.**
	
	Indicative content:
	
	The specification covers three areas:
	
	• Device forensics, eg:
	  o file systems
	  o extracting data from memory image
	  o hex editor or other specialised software
	  o cross referencing results from different tools to improve accuracy
	  o physical techniques, eg desoldering ('chip-off') and memory chip reader
	  o position data from GPS, deceleration data from airbag units.
	• Memory forensics, eg:
	  o memory dump
	  o visualisation techniques.
	• Network forensics, eg:
	  o security detection: anomalous traffic, intrusions
	  o law enforcement: analysis of traffic (reassembling transferred files, searching for keywords, parsing human communication, etc)
	  o brute force; intelligence-driven method.
	
	General approaches, eg:
	• Turn off/remove battery to preserve mobile data at a point in time.
	• Storage in appropriate conditions (dry, anti-static, secure etc).
	• Prevent contamination.
	• Isolate wireless devices.
	• Block writing to device/write blockers.
	• Back up data before analysis
	• Chain of custody, ie sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.
	
	Possible analytical techniques:
	• Cross drive analysis:
	  o correlates information found on multiple hard drives
	  o anomaly detection.
	• Live analysis:
	  o examination of computers from within the operating system
	  o using custom forensics or existing sysadmin tools to extract evidence.
	• Recovery of deleted files/file carving (from headers):
	  o recovering either whole or parts of
	  o operating systems don't usually erase files.
	• Stochastic forensics:
	  o randomly determined
	  o investigating data theft.
		12

Level	Descriptor	Marks
3	Clear explanations of a range of methods; accurate use of technical language and context.	9-12
2	Some explanation of methods, or describes a range of methods; mainly accurate use of technical language or context.	5-8
1	Lists methods with some attempt to describe; some accurate use of technical language or context	1-4
	No creditworthy response.	0

Total 15 Marks

Assessment Objectives									
Question	**AO1**	**AO2**	**AO3**	**AO4**	**AO5**	**AO6**	**AO7**	**AO8**	**Question Total**
Section A									
1	1a (1)								1
2								8b (1)	1
3			3d (1)						1
4		2b (1)							1
5	1a (1)								1
6.1						6c (2)			2
6.2						6c (2)			2
7.1		2b (1)							1
7.2		2b (3)							3
8	1c (4)								4
9.1		2b (2)							2
9.2		2b (4)							4
10	1b (3)								3
11				4a (2)					2
12.1							7a (4)		4
12.2					5b (4)				4
13.1			3c (4)						4
13.2			3c (4)						4
14.1				4a (2)					2
14.2				4a (2)					2
14.3				4a (2)					2
Section B									
15.1			3a (3)						3

15.2			3a (3)						3
15.3	1ab (2)	2ac (2)	3ef (2)	4b (1)	5ab (2)				9
16.1					5d (3)				3
16.2					5d (12)				12
Totals	11	13	17	9	21	4	4	1	**80**