Level 3 Technical Level

IT: CYBER SECURITY

Unit 6 Network and cyber security administration
J/507/6435
Report on the Examination

TVQ01009
January 2019

Version: 1.0

Further copies of this Report are available from aqa.org.uk

General

Students across all centres showed a willingness to engage with the questions and generally good examination technique, with most questions attempted and some evidence of planning answers.

Where an amount such as '**two** examples' is specified, and a student provides more than this amount, only the first two examples will be marked. Should a student change their mind, the redundant answers should be crossed out or otherwise made clear which two answers the student wishes to be considered.

Some students appeared to be running out of space to write, perhaps not aware that there were additional blank pages at the back to continue the answer. Future papers in all units will provide (or already have) more writing lines per question, though the additional pages will also be retained. Those with large handwriting, in particular, are urged not to treat the end of the writing space as an automatic end point for their answer and continue on the additional pages if it will add value to their response.

Responses to questions

Few students understood what hot/warm/cold sites were in the context of disaster recovery (AO6). Learners should be able to describe the differences and explain some of the options that might be included/excluded to balance system continuity/affordability. Some students included 'back-up generator' from this section of AO6 as part of Mrs Kumar's options for working from home but were evasive as to exactly what this was or how it might be used. For example, an uninterruptible power supply (UPS) might be used for a desktop computer but not usually for a laptop.

The specification includes legislation that an organisation needs to implement, such as to cover computer misuse or data protection. It would be expected that students could outline some differences between legislative acts such as the Computer Misuse Act and Data Protection Act / General Data Protection Regulation. Another area which required specific knowledge was the Cain and Abel password recovery tool and cryptanalysis.

Students understood what logs and data fields might be useful to a network manager but were less confident in explaining **how** the network manager could use that data in his/her everyday work. While the specification refers more specifically to organisations, understanding some of the roles within the organisation might be a useful starting point from which to develop understanding of how an organisation manages risk (AO2) and the situational awareness around Internet threats (AO5).

Most students had some idea what is meant by 'phishing' but many students referred to 'sending a deceptive email' without explaining what made it deceptive and/or the (fraudulent) objective of sending the email.

Sometimes the context given in the stem of the question was ignored. For example, if using biometric data to authenticate a user, it is probably not practical to use DNA. Students will not be credited for repeating material used in the stem of the question, in this case 'fingerprint' as an example of a biometric characteristic.

Many students showed an ability to develop their answers in Section B, focusing on different ways in which a scenario could be tackled and guiding themselves effectively by underlining key words in the questions. Students who were less successful tended to ignore parts of the bullets — or

even a bullet entirely — or, for the lead-in question (17.1), rehash similar reasons without articulating why the guideline would help **prevent** a virus attack in the first place.