Oxford Cambridge and RSA

Cambridge Technicals

IT

Level 2 Cambridge Technicals Certificates in IT **05883**

Level 2 Cambridge Technicals Diplomas in IT **05884**

OCR Report to Centres June 2018

About this Examiner Report to Centres

This report on the 2018 Summer assessments aims to highlight:

- areas where students were more successful
- main areas where students may need additional support and some reflection
- points of advice for future examinations

It is intended to be constructive and informative and to promote better understanding of the specification content, of the operation of the scheme of assessment and of the application of assessment criteria.

Reports should be read in conjunction with the published question papers and mark schemes for the examination.

The report also includes links and brief information on:

- A reminder of our **post-results services** including **reviews of results**
- Link to **grade boundaries**
- **Further support that you can expect from OCR**, such as our CPD programme

Reviews of results

If any of your students' results are not as expected you may wish to consider one of our Reviews of results services. For full information about the options available visit the OCR website. If University places are at stake you may wish to consider priority service 2 reviews of marking which have an earlier deadline to ensure your reviews are processed in time for university applications: http://www.ocr.org.uk/administration/stage-5-post-results-services/enquiries-about-results/service-2-priority-service-2-2a-2b/

Grade boundaries

Grade boundaries for this, and all other assessments, can be found on the OCR website .

Further support from OCR

CPD Hub
Your route to OCR's teacher training

Attend one of our popular CPD courses to hear exam feedback directly from a senior assessors or drop in to an online Q&A session.

https://www.cpdhub.ocr.org.uk

CONTENTS

Cambridge Technicals

Level 2 Cambridge Technical Certificate in IT 05883

Level 2 Cambridge Technical Introductory Diploma in IT 05884

OCR REPORT TO CENTRES

Unit 1 Essentials of IT

This is the second series where a test variant was sat by learners with varying performance across the five Learning Outcomes (LOs). As well as focusing on the knowledge requirements for this unit, centres should also ensure learners are familiar with the different assessment styles used in the summative assessment – i.e. linking boxes; true/false; diagram-related questions and select 'three'.

Learning Outcome 1

Having reported that this was weakest performing LO in January 2018, it was pleasing to note that this is now the strongest area. Centres have clearly invested some time in ensuring learners are familiar with hardware components. The vast majority of learners got the correct answer on items 1, 3, 8, 9, 11, 32 and 39 whilst items 20 and 31 proved more discriminating.

Learning Outcome 2

Performance on this LO has declined from January 2018. Only items 16, 37 and 38 were accessed by the majority of candidates. The remaining seven LO2 items proved more discriminating with items 5, 13 and 23 posing a real challenge for learners. Centres need to be aware that focusing on LO1 and LO2 knowledge requirements is time well spent. Scoring a healthy return of marks on these two LOs goes a long way to securing an overall 'Achieved' for this unit.

Learning Outcome 3

The same commentary as provided in January 2018 applies here. Performance on this LO which builds on LO1 and L02 was distinctly average. Of particular concern were items 24, 25, 26 and 33 which posed real issues for learners. Centres should ensure the gaps in LO1 (hardware) and LO2 (software) are addressed so learners have the best possible opportunity to succeed on this LO.

Learning Outcome 4

An LO which focuses on the use of the world-wide web is always predicted to generate a good level of performance, particularly given learners are digital users on a daily basis and have some inbuilt familiarity with the specification content. Items 10, 19, 27 and 28 were particularly strong whilst items 21, 22, 34 and 35 proved more discriminating.

Learning Outcome 5

This LO pulls the specification content of the unit together as learners are expected to reflect on the practical uses of IT within business. In contrast to January 2018, performance on this LO has improved this series with the vast majority of learners getting the correct answer for items 14, 15 and 29. Items 30 and 36 proved more discriminating.

Centres are advised for future series to maintain the good performance on LO1 whilst spending some time filling any knowledge gaps on the remaining four LOs. A particular focus needs to be LO3 as this was the weakest LO this series.

Unit 2 Essentials of Cyber Security

General Comments:

Many candidates demonstrated knowledge gaps in relation to the unit content. Centres should ensure that candidates are familiar with all areas of the unit content prior to being entered for the external examination.

The correlation between content, context and command word also appeared to be limited. Candidates should be aware of the differing command words, e.g. identify, describe, explain, discuss, and the demands of each of these and how these command words require different depths of response.

Comments on Individual Questions:

Q1a The focus of this question was on the different targets for cyber security attacks and ties into the list given in section 1.3 of the specification. Candidates frequently gave organisation, which was eliminated by the question.

Q1b This was generally done very well with the majority of candidates identifying phisher as the type of attacker.

Q1c This question focused on part 1.4 of the specification. Of the four types of cyber security incidents, two involve data loss. The majority of candidates were able to identify at least one of the incident types.

Q2a It was disappointing that candidates were not aware of the data protection act –many gave computer misuse or a combination of words from different acts.

Q2b The focus of the question was on access rights and how they improve security. Many of the responses from candidates ignored this aspect and gave details about how security could be improved with the application of passwords, achieving no marks. It is important that time is spent by the candidate reading the question.

Q2c The difference between a physical and a logical security measure was not appreciated by the majority of candidates with answers given that were not related to physical security.

Q2d The types of threats are given in section 2.1 of the specification. Few candidates could give the one related to individuals. Without correct identification of the threat, the descriptive marks could not be obtained.

Q2e This question is at the core of cyber security, why we need to protect personal data and it was disappointing that the majority of candidates did not have an appreciation or understanding of this core aspect of the specification.

Q3a The stem of the question gives some background to this question and its associated parts. One key piece of information is that the school has usernames and passwords currently in place. The focus of the question is on why they should increase the security. Many candidates gave responses based on security that could be applied, which in lots of cases included the use of passwords.

Q3bi The questions was asking for additional authentication that could be implemented, in addition to usernames and passwords. This was another question, which was not read by the candidates, and procedures based around passwords were given, including details on increasing complexity of passwords, which gained no marks.

Q3bii The identification aspect of this question was answered reasonably well by many candidates, however few went on to give adequate descriptions.

Q3ci This question focused on part 1.4 of the specification. Of the four types of cyber security incidents, two involve data modification. Unfortunately, few candidates were able to identify these incident types.

Q3cii This question is ties into the correct identification of the incident type. Without correct answers being obtained in Q3ci, marks cannot be obtained for this question. If the incidents were correctly identified, the candidates were being asked to apply their knowledge to the scenario given in the question. Whilst many used terms associated with schools, few were able to give specific examples that met the marking criteria.

Q3di The focus of this question was twofold – organisational and intentional. Most candidates correctly identified hacking as one of the acceptable types, but often the expansion was lacking detail.

Q3dii This question required the candidates to give an additional threat. Unfortunately, the majority of candidates only knew one threat and had given this in Q3di.

Q3e This question was marked using a banded response method. Candidates were awarded marks based on the level of detail included in their response, and the application of their response to scenario. The question focused on the vulnerabilities that could lead to a cyber security attack – as this is part of question 3, it continues from the stem and hence the procedures that are currently in place. Therefore, responses relating to need for passwords gained no marks.

There are four main areas – environmental, physical, personnel and system with a variety of vulnerabilities that could have been discussed. The keyword discuss requires, for the top mark band, the candidates to show a detailed level of understanding by explaining the vulnerabilities which could occur. They would need to explain more than one vulnerability. There is also an expectation that relevant and appropriate examples are used by the candidate. Those candidates who did give suitable vulnerabilities often failed to give suitably detailed explanations. Many candidates took the “scattergun” approach, listing as many vulnerabilities as they know without giving the depth and detail required for each to move through the bands.

About OCR

OCR (Oxford Cambridge and RSA) is a leading UK awarding body. We provide qualifications which engage people of all ages and abilities at school, college, in work or through part-time learning programmes.

As a not-for-profit organisation, OCR's core purpose is to develop and deliver general and vocational qualifications which equip learners with the knowledge and skills they need for their future, helping them achieve their full potential.

OCR (Oxford Cambridge and RSA Examinations)
The Triangle Building
Shaftesbury Road
Cambridge
CB2 8EA

OCR Customer Contact Centre

Telephone: 02476 851509
Facsimile: 02476 421944
Email: vocational.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