

CAMBRIDGE TECHNICALS LEVEL 3 (2016)

Examiners' report

IT

05838–05842, 05877

Unit 3 Summer 2023 series

Contents

Introduction3

Unit 3 series overview4

Section A overview5

 Question 1 (a) (i)5

 Question 1 (a) (ii)5

 Question 1 (b)6

 Question 2 (a) (i)6

 Question 2 (a) (ii)7

 Question 2 (b)*7

 Question 2 (c)*8

 Question 3 (a)9

 Question 3 (b) (i)9

 Question 3 (b) (ii)10

 Question 3 (b) (iii)11

 Question 3 (c)11

Section B overview12

 Question 4 (a) (i)12

 Question 4 (a) (ii)12

 Question 4 (b) (i)12

 Question 4 (b) (ii)13

 Question 5 (a)13

 Question 5 (b)14

 Question 5 (c)14

 Question 6 (a)15

 Question 6 (b)15

Introduction

Our examiners' reports are produced to offer constructive feedback on candidates' performance in the examinations. They provide useful guidance for future candidates.

The reports will include a general commentary on candidates' performance, identify technical aspects examined in the questions and highlight good performance and where performance could be improved. The reports will also explain aspects which caused difficulty and why the difficulties arose, whether through a lack of knowledge, poor examination technique, or any other identifiable and explainable reason.

Where overall performance on a question/question part was considered good, with no particular areas to highlight, these questions have not been included in the report.

A full copy of the question paper and the mark scheme can be downloaded from OCR.

Would you prefer a Word version?

Did you know that you can save this PDF as a Word file using Acrobat Professional?

Simply click on **File > Export to** and select **Microsoft Word**

(If you have opened this PDF in your browser you will need to save it first. Simply right click anywhere on the page and select **Save as . . .** to save the PDF. Then open the PDF in Acrobat Professional.)

If you do not have access to Acrobat Professional there are a number of **free** applications available that will also convert PDF to Word (search for PDF to Word converter).

Unit 3 series overview

This unit is mandatory for the Extended Certificate, Diploma and Extended Diploma and optional for all pathways for the Introductory Diploma and Foundation Diploma.

The unit focuses on:

- an understanding of cyber security and the issues surrounding it
- measures that can be used to protect against cyber security incidents
- an understanding of how to manage cyber security incidents.

The paper is divided into two sections – A and B. Section A is worth 60% (40 marks) and is based around a pre-release scenario. The pre-release contains areas for further research that the candidate is expected to undertake, and which form the basis of the questions to be asked. Section B is worth 40% (20 marks) and each question has its own short scenario.

| Candidates who did well on this paper generally: | Candidates who did less well on this paper generally: |
|---|---|
| <ul style="list-style-type: none"> • used technical terms • related their responses to the scenario in the question • used the keywords in the question to give appropriate depth to their responses • knew the key definitions from the specification. | <ul style="list-style-type: none"> • answered the question they thought was being asked, not the one actually being asked • repeated the same point several times in different ways • gave an answer that had been eliminated in the question. |

Section A overview

The pre-release identifies key research topics that the candidates should have spent some time working on. They needed to have cross referenced the topics against the specification.

Question 1 (a) (i)

1 (a) Pen Perimeter has been hired by a government department to report on the security of the data it stores.

(i) Describe **one** type of state's data that needs to be **protected**.

.....
.....
.....
..... [2]

This question followed on from the pre-release and required a regurgitated knowledge based response. The key was that the data had to relate to the state and not generic personal information.

Question 1 (a) (ii)

(ii) Identify **one other** type of state's data that needs to be **protected**.

.....
..... [1]

Some candidates repeated their response from Question 1(a)(i) so were not given the mark. Many could not identify a second type of state's data – this is given in the specification and was highlighted as a requirement in the pre-release.

Question 1 (b)

(b) One of Pen Perimeter’s clients is a healthcare provider.

Identify **two** reasons why an organisation, such as a healthcare provider, might be a **target** for a cyber security threat.

Reason 1

.....

Reason 2

.....

[2]

The focus is on why an organisation would be a target. Many responses did identify the fact that they held different types of data and some more original reasons based around medical research were also given marks.

Question 2 (a) (i)

2 Pen Perimeter carried out tests for a charity.

A Test Report was created which included recommendations for improvements for the charity’s cyber security.

(a) (i) Identify **three different physical** based cyber security controls that Pen Perimeter would have tested.

Control 1

.....

Control 2

.....

Control 3

.....

[3]

This was very well answered by the majority of candidates. Where they did not score highly was when they confused physical and logical.

Question 2 (a) (ii)

- (ii) Identify **two different software** based cyber security controls that Pen Perimeter would have tested.

Control 1

.....

Control 2

.....

[2]

This was very well answered by the majority of candidates. Where they did not score highly was when they confused software based with physical.

Question 2 (b)*

- (b)* Using examples, explain how the cost of implementing the recommendations of the report could **outweigh** the benefits.

.....

.....

.....

.....

.....

.....

.....

[7]

There are many different aspects that constitute costs that go beyond money. The majority of responses were in the lower band because the answer was essentially it costs a lot of money, without giving detail or explanation. Even though 'outweigh' was emboldened, some candidates appeared to have misread the question and gave reasons why the recommendations should be implemented and the benefits of doing so.

Misconception



Essays are marked using bands and not using points. This means that the candidate needs to be making a few points, and each point needs to show the depth of their knowledge and understanding, rather than making many points which demonstrate a superficial breadth. A discussion requires an explanation, backed up with examples relevant to the question. The explanation needs to make up the majority of the response, rather than be added as an afterthought.

Question 2 (c)*

(c)* Discuss the implications for **stakeholders** of the charity if they did **not** act on the recommendations of the report.

.....

.....

.....

.....

.....

.....

..... **[10]**

This essay question elicited a greater range of responses from the candidates than the previous one. Many candidates applied the negative implications to the charity as a whole and this level of application and discussion allowed them to achieve marks in the top band.

Too many responses however were a list of points that were not explained or exemplified, which limited the marks that could be given.

Question 3 (a)

3 Pen Perimeter has been hired by a financial business to carry out a simulated cyber security attack on their network.

(a) After containing the incident, the financial business needs to **eradicate** it.

Identify **two** ways the incident could be **eradicated**.

Way 1

.....

Way 2

.....

[2]

The stages of dealing with a cyber security incident are laid out in the specification. Eradication is an important stage and involves the removal of the cause of the incident. Too many responses gave impractical and incorrect responses relating to switching off equipment, rebuilding from backups and deleting files. These would not have removed the cause of the incident. The majority of the correct responses focused on a type of incident, for example, a virus and then gave steps to how it could be removed.

Question 3 (b) (i)

The financial business uses the attack to practise its production of a cyber security incident report.

(b) (i) Why is it important to understand if the **target** of the incident was a particular department or individual?

.....

.....

.....

..... [2]

The key to the question was being able to say why it was important. This is related to the response that would be initiated.

A high percentage of responses tried to give examples of how the target could be identified or what the target would need to do if they suspected an incident.

Question 3 (b) (ii)

(ii) The incident is given a category.

Draw a line to match **each** incident category to the correct definition.

| | |
|-------------|---|
| Critical | Inconvenient, loss of efficiency but able to provide services. |
| Minor | Loss of reputation, disruption to services, financial loss. |
| Significant | Organisation is no longer able to provide some critical services to users, lives may be lost. |
| | Minimal impact on systems, services and users. |

[3]

This was generally well done with most responses being given high marks. Some responses lost marks for trying to link the category to more than one definition.

Question 3 (b) (iii)

(iii) Describe **two different** ways the capability of the attackers could be **established**.

Way 1

.....

.....

.....

Way 2

.....

.....

.....

[4]

This was generally well answered with techniques used being the common correct answer. However, many candidates did not describe their answer, only identified, and so did not secure the subsequent mark. A list of different techniques could not be given marks beyond the identification of the first one.

Question 3 (c)

(c) After the incident the financial business **updates** its documentation.

Identify **two different** items of documentation it would **update** to assist in future cyber security attacks.

Item 1

.....

Item 2

.....

[2]

The important part of this question was the use of the documentation for future attacks. This means that it needs to be documentation that are updated after that incident and used to prepare for future ones. Cyber Security Incident Reports are completed while the incident is ongoing and so could not be given the mark.

The majority of correct responses focused on training, policies, and procedures.

Section B overview

This section is not based on the pre-release material. Each question is given a short context and candidates are expected to use it, where appropriate, within their responses.

Question 4 (a) (i)

4 (a) (i) What does **confidentiality** of information mean?

.....
..... [1]

This was answered very well with the majority gaining the mark.

Question 4 (a) (ii)

(ii) Identify **two** measures that can be implemented to ensure the **confidentiality** of information.

Measure 1
.....
Measure 2
..... [2]

The majority of candidates were able to identify two measures.

Question 4 (b) (i)

(b) (i) What does **integrity** of information mean?

.....
..... [1]

This was answered very well with the majority gaining the mark.

Question 4 (b) (ii)

(ii) Identify **two** measures that can be implemented to ensure the **integrity** of information.

Measure 1

.....

Measure 2

.....

[2]

Few responses gave two methods for ensuring integrity. A few gave one method, but many gave a similar or the same method they gave for confidentiality.

Question 5 (a)

5 (a) Identify **two** motivations of a cyber-criminal.

Motivation 1

.....

Motivation 2

.....

[2]

Financial in all its variants was the most common response. As a criminal, the motivation needed to match, and this was where candidates needed to take all the motivations they knew and decide which were relevant. Fun, for example, was not relevant in this instance.

Question 5 (b)

- (b) For each cyber security incident, identify the **type of attacker** who would most likely be involved.

| Cyber Security Incident | Type of Attacker |
|--|------------------|
| Changing grades in a school | |
| Employee releasing customer information to a rival firm | |
| Hacking a company and releasing information on salary gender imbalance | |

[3]

This was generally done very well with the majority gaining most of the marks.

Question 5 (c)

- (c) One of the targets for cyber security incidents is **information**.

Explain how a hacker could use **information** about an individual obtained from a cyber security incident.

.....

.....

.....

.....

.....

.....

..... [3]

Candidates scored highly on this question. The majority of the responses were based around identity theft and finances. There was some evidence of explanation as to how the information could be used and its impact on the individual which was pleasing to see.

Question 6 (a)

6 (a) Explain how **encryption** can be used to protect data.

.....

.....

.....

.....


.....

.....

..... [3]

There were many unsuccessful responses to this question. Along with saying that encrypted text could not be read, many did not give the technical detail of how encryption protects data and so the responses given lacked depth.

Misconception

 A common misconception is that encryption makes the data unreadable. The data is still readable, but meaningless.

Question 6 (b)

(b) Describe characteristics of **physical** cyber security controls that make them suitable for preventing cyber security incidents.

.....

.....

.....

.....

.....

..... [3]

This was not answered well. Many answered the question by listing physical cyber security controls and then went on to give a description of how they worked, rather than focus on the suitability of the control for preventing incidents.

Supporting you

Teach Cambridge

Make sure you visit our secure website [Teach Cambridge](#) to find the full range of resources and support for the subjects you teach. This includes secure materials such as set assignments and exemplars, online and on-demand training.

Don't have access? If your school or college teaches any OCR qualifications, please contact your exams officer. You can [forward them this link](#) to help get you started.

Reviews of marking

If any of your students' results are not as expected, you may wish to consider one of our post-results services. For full information about the options available visit the [OCR website](#).

Keep up-to-date

We send a monthly bulletin to tell you about important updates. You can also sign up for your subject specific updates. If you haven't already, [sign up here](#).

OCR Professional Development

Attend one of our popular CPD courses to hear directly from a senior assessor or drop in to a Q&A session. Most of our courses are delivered live via an online platform, so you can attend from any location.

Please find details for all our courses for your subject on **Teach Cambridge**. You'll also find links to our online courses on NEA marking and support.

Signed up for ExamBuilder?

ExamBuilder is the question builder platform for a range of our GCSE, A Level, Cambridge Nationals and Cambridge Technicals qualifications. [Find out more](#).

ExamBuilder is **free for all OCR centres** with an Interchange account and gives you unlimited users per centre. We need an [Interchange](#) username to validate the identity of your centre's first user account for ExamBuilder.

If you do not have an Interchange account please contact your centre administrator (usually the Exams Officer) to request a username, or nominate an existing Interchange user in your department.

Need to get in touch?

If you ever have any questions about OCR qualifications or services (including administration, logistics and teaching) please feel free to get in touch with our customer support centre.

Call us on
01223 553998

Alternatively, you can email us on
support@ocr.org.uk

For more information visit

 **ocr.org.uk/qualifications/resource-finder**

 **ocr.org.uk**

 **facebook.com/ocrexams**

 **twitter.com/ocrexams**

 **instagram.com/ocrexaminations**

 **linkedin.com/company/ocr**

 **youtube.com/ocrexams**

We really value your feedback

Click to send us an autogenerated email about this resource. Add comments if you want to. Let us know how we can improve this resource or what else you need. Your email address will not be used or shared for any marketing purposes.



I like this



I dislike this

Please note – web links are correct at date of publication but other websites may change over time. If you have any problems with a link you may want to navigate to that organisation's website for a direct search.



OCR is part of Cambridge University Press & Assessment, a department of the University of Cambridge.

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored. © OCR 2023 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 operates academic and vocational qualifications regulated by Ofqual, Qualifications Wales and CCEA as listed in their qualifications registers including A Levels, GCSEs, Cambridge Technicals and Cambridge Nationals.

OCR provides resources to help you deliver our qualifications. These resources do not represent any particular teaching method we expect you to use. We update our resources regularly and aim to make sure content is accurate but please check the OCR website so that you have the most up to date version. OCR cannot be held responsible for any errors or omissions in these resources.

Though we make every effort to check our resources, there may be contradictions between published support and the specification, so it is important that you always use information in the latest specification. We indicate any specification changes within the document itself, change the version number and provide a summary of the changes. If you do notice a discrepancy between the specification and a resource, please [contact us](#).

You can copy and distribute this resource freely if you keep the OCR logo and this small print intact and you acknowledge OCR as the originator of the resource.

OCR acknowledges the use of the following content: N/A

Whether you already offer OCR qualifications, are new to OCR or are thinking about switching, you can request more information using our [Expression of Interest form](#).

Please [get in touch](#) if you want to discuss the accessibility of resources we offer to support you in delivering our qualifications.