CAMBRIDGE TECHNICALS

OCR
Oxford Cambridge and RSA

CAMBRIDGE TECHNICALS LEVEL 3 (2016)

Examiners' report

IT

05838–05842, 05877

Unit 3 January 2025 series

Contents

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 Teach Cambridge.

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 are 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:
• used technical terms • related their answers to the scenario in the question • used the keywords in the question to give appropriate depth to their response • learnt the key definitions from the specification.	• 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 has 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 need to have cross referenced the topics against the specification. The pre-release material assists the candidates in what to study and can be used to give an insight into the answers to certain questions.

Question 1 (a)

Triangle Widgets is conducting a review into its cyber security.

1 The first stage in the review is to identify vulnerable assets.

(a) Identify **two** different **assets** Triangle Widgets has that could be the target of a cyber security incident.

Asset 1 .....

.....

Asset 2 .....

.....

[2]

An understanding of the assets that could be attacked is fundamental to cyber security and this was the first further research theme candidates were asked to complete in the pre-release.

Generally, this question was done well with candidates identifying two different assets. Marks were lost where candidates gave the same asset in two different ways.

Question 1 (b)

(b) Describe how the risk to Triangle Widgets can be analysed if an asset is compromised.

.....

.....

.....

.....

.....

..... **[4]**

Candidates were asked to analyse risk in the pre-release, so it was disappointing that this was not done particularly well. Candidates often focused on how the asset could have been compromised and then what needed to be done to prevent this from happening in the future. The question was about how to analyse the risk not to prevent it. In the context of the question paper the risk has already been compromised, and it is working out how the risk is analysed that was being asked.

Question 2 (a)

As part of the review, the Triangle Widgets is looking at how its cyber security can be improved.

2 One area of improvement is the introduction of new security measures and controls.

(a) Describe **two operational** considerations Triangle Widgets needs to consider when implementing new security measures and controls.

Consideration 1 .....

.....

.....

.....

Consideration 2 .....

.....

.....

.....

[4]

Candidates needed to identify and describe two operational considerations. The control is being implemented – this means that a decision has been made, and the control purchased. Cost is therefore not a factor; this is about how to take the control and make it work on a day-to-day basis in the organisation. This directly linked to research theme 2 in the pre-release. Generally, this was done poorly with candidates not reading the question or applying their research from the pre-release themes.

Question 2 (b)

The review has identified that Triangle Widgets should install an intrusion prevention system (IPS).

(b) Explain **two** features of an **intrusion prevention system (IPS)** that Triangle Widgets can use to improve its cyber security.

Feature 1 .....

.....

.....

.....

Feature 2 .....

.....

.....

.....

[4]

The was done reasonably well by many candidates. Those who did not score highly gave very generalised answers that lacked any technical detail or understanding or gave answers that were specifically about antivirus software or firewalls.

Question 2 (c)

The review has identified that Triangle Widgets should use device management.

(c) Explain how Triangle Widgets can use **device management** to improve its cyber security.

.....

.....

.....

.....

.....

..... **[3]**

There was confusion among candidates over device management, software management and access control. Many answers included elements of all of them. While some candidates know what device management was, they did not relate it to how it could improve cyber security, losing marks. Answers needed to focus on the use of the device to be credited, vague answers related to not allowing the machine off premise did not explain how device management was being used.

Question 2 (d)

The review has identified that Triangle Widgets has a number of staff who work remotely and this is an area for concern.

(d) Explain why **remote working** is a concern for cyber security for Triangle Widgets.

.....

.....

.....

.....

.....

..... **[3]**

This was generally well answered with many candidates focusing on the use of own devices and shoulder surfing. There was an obsession with the inability to monitor devices coming through from many candidates.

Question 3 (a)

3 As part of the review Triangle Widgets is looking into how it would react if it was the victim of a cyber security incident. Triangle Widgets is running a table top exercise simulating the release of all its customers' personal details.

(a) Describe **two** actions Triangle Widgets can take to reduce the **impact** of this cyber security incident on its **customers**.

Action 1 .....

.....

.....

.....

Action 2 .....

.....

.....

.....

[4]

The tabletop exercise is in progress, customer details have been released, and the focus of the question was on the impact on customers. Many answers focused on how the attack could have been prevented, how it could be prevented in the future or what the organisation should do to protect itself. Very few candidates read the introduction to the question and thought about that the question was asking. There were too many pre-prepared responses that did not consider the next steps required.

Question 3 (b)

The cyber security incident needs to be categorised.

(b) Identify the **four** types of **incident category**.

Type 1 .....

.....

Type 2 .....

.....

Type 3 .....

.....

Type 4 .....

.....

[4]

As a learnt response this was either known or not know. It was not possible to guess at the answers.

Question 3 (c)

One external authority that would need to be informed of the cyber security incident is the police.

(c) Identify **two other** external organisations that would need to be informed of the cyber security incident.

For **each** organisation, explain why they need to be informed.

Organisation 1 .....

Why informed .....

.....

Organisation 2 .....

Why informed .....

.....

[4]

It was disappointing to see candidates giving police as an answer when it was specifically eliminated by the question. Many candidates also gave 'organisations' that were either not organisations – such as customers or stakeholders or were into external to the company – employees for example. The ICO, or a variant was the most common correct answer given. There were also a few American organisations given that also gained credit.

Question 4*

Information has been received from the police of specific cyber security attacks against other companies in the same industry across the globe.

4* Discuss the impacts that cyber security incidents can have as a **global problem**.

.....

.....

.....

.....

.....

..... **[7]**

There were two elements to this question, the impact of a cyber security incident and the global issue. Many candidates gave impacts of incidents although few explained them, with many limited their response to descriptions. Attempted explanations usually were single words or phrases, such as bankrupt, loss of customers or loss of trust with no depth. The main issue with the responses was that their reference to global was often added as an after though at the end of the essay and the main content of their response does not have any relevance to a cross border/global issue.

Assessment for learning

There are two essays in the paper, one worth 7 marks and one worth 10 marks. These are marked using a level of response mark scheme rather than point marked with the levels being determined by the depth of the candidate's response. Essays such as this require depth of response from the candidate rather than breadth. A few points are required but the candidate is required to show their understanding of the point and its application to the question.

Formatting the response can assist this, with each point being made being a separate paragraph; this can help focus the candidate on the point being made rather than moving onto a different one and reducing the depth of their argument and marks given.

The use of the highlighter to identify the key points in the question is a technique that has been seen used to great effect.

Exemplar 1

Organisations, such as Triange Widgets, often have supply-chains and other organisations they work ~~for~~ with located in different countries. Since these organisations are all connected, it's easy for a cyber security incident to propogate through them. This ~~can~~ ~~propogate~~ results in many organisations in different countries being compromised. // Due to regulations in different countries, Triangle Widgets would have to, potentially, pay ~~fines~~ several fines to different countries. This could end up costing a large amount of money, which may damage Triangle Widget's business. Consequently, they may not be able to work with those other organisations anymore due to costs. That could then damage those companies as they're losing out on money, which could impact that industry globally. // Furthermore, if data is stolen as part of the cyber security attack, this could also have a devastating effect on organisations linked with Triangle Widgets. If data such as bank details are stolen, the cyber criminal can exploit this and ~~take~~ steal money from the organisations. This could damage several of those ~~ego~~ organisations, having a global impact, and ~~could~~ would also lead to a loss of ~~the~~ trust in Triangle Widgets. This may mean that they won't work together anymore, potentially damaging the industry globally. **[7]**

As can be seen in the script included here, the candidate has attempted to tie their response into the global element – organisations with supply chains in different countries, ease by which a cyber security incident can cross boundaries and the idea of data protection violations in different countries adding up with fines. There are some impacts identified and some of these have started to be developed – not working with the companies anymore, loss of trust however these are not developed nor explained which limits them to a maximum of 5/7.

Section B overview

This section is not based on the pre-release material. There is a stem to the section and candidates are expected to use it, where appropriate, within their responses.

Question 5*

5* Explain why an individual needs to protect their personal data.

.....

.....

.....

.....

.....

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

This was quite a wide essay which allowed the candidate to demonstrate their knowledge and understanding of cyber security. The starting point for the better essay was the CIA triad which underpins the cyber security specification and then these were developed in relation to the protection of personal data. Most candidates identified why individuals need to protect their data with identity theft being one of the most common reasons given, but as there was no depth or detail to their answers, they did not score more than 3. A list of reasons is not enough to take candidates beyond the first band.

Exemplar 2

An individual needs to protect their personal data so that they can remain safe. If an attacker were to find out where someone lived who they deemed vulnerable. They may take advantage of that and go an steal from them / attacle them with. Therefore, keeping personal data, such as your address, safe, protects you from physical harm.

An individual also needs to protect their personal data so that they aren't a victim of blackmail. If an attacker were to gain access to embarrassing information about an individual, they could use that against them. Therefore, it is essential that personal data is protected so that this cannot happen.

Furthermore, if an attacker were to gain access to personal data such as bank details, this puts the individual's money at risk. The attacker may then be able to steal money, take out loans and mortgages in their name, and close / open new accounts. This could result in a loss of money and a poor credit score, potentially leading to banks not wanting to work with them and an inability to take out loans / mortgages in the future. Therefore, personal data must be protected. **[10]**

As can be seen in the script included here, the candidate has identified and added some description but there is a lack of detail of explanation – it is mostly limited to phrases such as 'protecting from physical harm ', 'use against them', 'loss of money'. The final paragraph does look at loss of money in more detail – banks not wanting their custom and this having an impact on loans and mortgages. While not a detailed explanation, it is an impact that has logical consistency with their previous points and is enough to tip them into the top band giving them a mark of 7/10.

Question 6 (a)

6 There has been an increase in the number of online cyber security attacks.

One type of attackers are hacktivists.

(a) Explain **one** target a hacktivist could attack.

.....

.....

.....

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

This was looking to see if the candidate understood hacktivist and how they are different from the other types of attackers listed in the specification. This was generally done well with candidates giving examples of targets. Candidates who gave criminal based targets did not achieve marks.

Question 6 (b)

Another type of attackers are insiders.

(b) Describe **two** motivations for an **insider**.

Motivation 1 .....

.....

.....

.....

Motivation 2 .....

.....

.....

.....

[4]

The types of motivation are listed in the specification and are very specific. This was a learnt response – could the candidate identify the motivation from the type of attacker.

Misconception

Once an insider resigns or is fired and is no longer employed by the company, then they cease to be an insider.

Question 6 (c)

(c) Describe **two methods** that could be used by an attacker to target a person to gain information that could be used to access their online accounts.

Method 1 .....

.....

.....

.....

Method 2 .....

.....

.....

.....

[4]

The identification of methods that could be used was generally well done by candidates. Their description of the method was not done as well with many only scoring half marks.

Question 6 (d)

A person is one type of target for cyber security threats.

(d) Identify **one other** type of target.

.....

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

The types of targets are listed in the specification and are very specific and it was good to see most candidates achieving this mark.

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.

Online courses

Enhance your skills and confidence in internal assessment

What are our online courses?

Our online courses are self-paced eLearning courses designed to help you deliver, mark and administer internal assessment for our qualifications. They are suitable for both new and experienced teachers who want to refresh their knowledge and practice.

Why should you use our online courses?

With these online courses you will:

- learn about the key principles and processes of internal assessment and standardisation
- gain a deeper understanding of the marking criteria and how to apply them consistently and accurately
- see examples of student work with commentary and feedback from OCR moderators
- have the opportunity to practise marking and compare your judgements with those of OCR moderators
- receive instant feedback and guidance on your marking and standardisation skills
- be able to track your progress and achievements through the courses.

How can you access our online courses?

Access courses from Teach Cambridge. Teach Cambridge is our secure teacher website, where you'll find all teacher support for your subject.

If you already have a Teach Cambridge account, you'll find available courses for your subject under Assessment - NEA/Coursework - Online courses. Click on the blue arrow to start the course.

If you don't have a Teach Cambridge account yet, ask your exams officer to set you up – just send them this link and ask them to add you as a Teacher.

Access the courses **anytime, anywhere and at your own pace**. You can also revisit the courses as many times as you need.

Which courses are available?

There are **two types** of online course: an **introductory module** and **subject-specific** courses.

The introductory module, Building your Confidence in Internal Assessment, is designed for all teachers who are involved in internal assessment for our qualifications. It covers the following topics:

- the purpose and benefits of internal assessment
- the roles and responsibilities of teachers, assessors, internal verifiers and moderators
- the principles and methods of standardisation
- the best practices for collecting, storing and submitting evidence
- the common issues and challenges in internal assessment and how to avoid them.

The subject-specific courses are tailored for each qualification that has non-exam assessment (NEA) units, except for AS Level and Entry Level. They cover the following topics:

- the structure and content of the NEA units
- the assessment objectives and marking criteria for the NEA units
- examples of student work with commentary and feedback for the NEA units
- interactive marking practice and feedback for the NEA units.

We are also developing courses for some of the examined units, which will be available soon.

How can you get support and feedback?

If you have any queries, please contact our Customer Support Centre on 01223 553998 or email support@ocr.org.uk.

We welcome your feedback and suggestions on how to improve the online courses and make them more useful and relevant for you. You can share your views by completing the evaluation form at the end of each course.

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
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.

CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT