CAMBRIDGE TECHNICALS

OCR
Oxford Cambridge and RSA

Examiners' report

CAMBRIDGE TECHNICALS LEVEL 3 (2016)

IT

OCR Level 3 Cambridge Technical in IT

Certificate: 05838

Extended Certificate: 05839

Introductory Diploma: 05840

Foundation Diploma: 05841

Diploma: 05842

Extended Diploma: 05877

Unit 3 Summer 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 topics 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 • learned 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)

1

(a) Identify **two** types of attackers that could have gained the information from PH Software.

Tick **two** boxes.

- Cyber criminal ☐
- Hacktivist ☐
- Phisher ☐
- Scammer ☐

[2]

Many candidates identified one of the attackers but struggled with the second. All section A questions are related to the scenario and pre-release which did not involve hacktivist or scammer.

Question 1 (b)

(b) Describe **one** characteristic of an **insider**.

.....

.....

.....

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

This question was linked to the first research bullet point - the types of attackers who would want to target PH Software including their characteristics and motivations. Candidates generally performed well on this question and achieve one mark but for many, they veered into motivations and so were not able to gain both marks.

Question 1 (c)

(c) Identify **two** possible motivations of the insider giving the information to a competitor.

1 .....

2 .....

[2]

This was very well answered by the majority of candidates achieving both marks.

Question 2 (a)

2

(a) Explain **two** reasons why PH Software needs to protect the code for its new applications.

1 .....

.....

.....

.....

2 .....

.....

.....

.....

[4]

This was the fifth research bullet point - why PH Software needs to protect its information. The focus was on the protection of the code but many candidates talked about GDPR, trust and reputation. The response required, as an explanation, needed detail to obtain all the marks and in many cases, this was lacking.

Question 2 (b)

(b) Describe **three** methods the insider could have used to obtain the confidential client information from PH Software.

1 .....

.....

.....

.....

2 .....

.....

.....

.....

3 .....

.....

.....

.....

[6]

This question was based on the second research bullet point - methods that the attacker could use to obtain information from PH Software. It was a poorly answered question with candidates focussed on hacking and social engineering and not able to describe the method in detail.

Question 2 (c)

(c) Explain **two** impacts to PH Software of its confidential client information being obtained by the insider.

1 .....

.....

.....

.....

2 .....

.....

.....

.....

[4]

This was based on the third research bullet point - the impact of an attack on PH Software. This was answered reasonably well by candidates – due in part to GDPR being one of the answers. Loss of trust and reputation (given by many candidates in question 2 (a)) were acceptable but the explanations lacked depth limiting the marks to two.

Question 2 (d)

(d) Identify **two** ways that PH Software could know which information the insider handed to its competitors.

1 .....

2 .....

[2]

This was not very well answered with most candidates only gaining one mark for identifying/looking at logs. Candidates focused heavily on missing or deleted files which was incorrect. A small number did gain marks for references to approaches by the rival company on customers and similarities in products.

Question 2 (e)*

(e)* Discuss how PH Software can use the cyber security incident to assist in its future management of cyber incidents.

.....

.....

.....

.....

.....

.....

[10]

This was research point six - how PH Software can use the attack in future planning, so it was disappointing that this was not done particularly well. The cyber security incident is an insider attack. Many candidates gave generic responses related to upgrading the security of the system or employing white hack hackers. Responses such as this did not use the cyber security incident from the pre-release and did not score marks. The flow of the paper and the questions so far are about insiders, so it was disappointing to see this part of the pre-release and the paper completely being ignored by candidates. Many demonstrated a good level of knowledge and understanding of the process of managing of cyber security incidents, but it was not contextualised.

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 in 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

PH Software could identify the threat of an insider and use this knowledge to use access rights. Access rights ensure that only ~~neccessary in~~ employees that need access have access. This could prevent future low-level insiders from causing the same damage as they would not have access. However, high-level insiders (e.g. network manager) would still be able to access personal information.

PH Software should use the incident to identify weaknesses in their response. For example, if a staff member that is crucial for incident response has a hybrid working contract, there is a chance that they might be unavailable for ~~physical~~ response during an incident due to a poor ~~connect~~ ~~con~~ connection. PH Software should mitigate this risk by spreading responsibility among staff or discouraging ~~hyb~~ hybrid working.

PH Software could train staff regarding the incident, reducing the chance of social engineering.

[10]

Turn over

As can be seen in the script for this question, the candidate has immediately understood that the cyber incident in question is about insiders. This sets the tone for the rest of the essay. Access rights are one aspect that could be changed for insiders, they also recognise that for individuals with a lot of access they cannot be stopped through this method. The hybrid working is mentioned in the pre-release and picked up here by the candidate – linked to availability and speed of response. The final paragraph is not entirely relevant, although social engineering – phishing attacks is one method by which an insider could get credentials to assist them in vertical escalation of privileges.

Overall, the candidate has discussed how PH software could use the incident in future management. There are examples related to PH Software and the case study. This places them in the top mark band (7-10). However, the points are not as well developed as they might and working from the top down, this gets 8/10.

Question 3*

3* Evaluate the effectiveness of an Intrusion Detection System (IDS) for preventing insider attacks.

.....

.....

.....

.....

.....

.....

[7]

Candidates should have research this as part of the pre-release. They were directed to look at different methods PH Software could use to prevent the attack and the effectiveness of those methods. Some candidates confused IDS and IPS. Others neglected the prevention of insider attacks and gave generic responses. Candidates who only focused on one side – either positives or negatives were unable to move beyond mark band two in the level of response.

Assessment for learning

A good understanding of examination technique is necessary to be able to identify how to answer the question. For example, an evaluate requires positive, negative and a conclusion. Time spent on keywords and their requirements can help candidates to focus their time and responses on areas that will gain marks.

Exemplar 2

3* Evaluate the effectiveness of an Intrusion Detection System (IDS) for preventing insider attacks.

An IDS would be useful for informing other employees of an attack occuring. This would allow them to take appropriate actions or contact others in order to prevent the incident from escalating or causing more damage.

However, an IDS does not stop the attacker from gaining access to confidential information and therefore if other employees are unable to take action against the attack, an insider could successfully steal data, and use it with malicious intent.

The effectiveness of an IDS preventing attacks depends on the availability of individuals, but it is not effective in stopping an attack just by itself.

[7]

As can be seen in the script for this question, the candidate has given a positive and a negative and finished with a conclusion. The structure of the essay allows marks in the top band to be accessed. The first paragraph focuses on informing and the fact that the software does not do the work, but other employees need to take action. The second paragraph is a negative explanation based on it not taking action. The view taken in conclusion is not important – there is not a right or wrong answer here, it is about the candidate making a justified decision – which they have done in this case. The content of their essay places them in the mark band 3 (5-7) with the conclusion placing them at the top of the mark band – 7/7.

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 4 (a) (i)

4
(a)
(i) What is meant by **availability**?

.....

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

This part of cyber security teaching content LO 1.1 – the CIA (Confidentiality, Integrity, Availability) triad was generally well answered.

Question 4 (a) (ii)

Ryan is concerned that their bank account is no longer confidential.

(ii) What is meant by **confidentiality**?

.....

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

Candidates answered this very well with most achieving the mark.

Question 4 (a) (iii)

Ryan fears the integrity of the bank account has been compromised.

(iii) What is meant by **integrity**?

.....

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

While many were able to gain the mark, there was a disconcerting number who took the English language approach to the term and gave a generic non ICT based meaning. The CIA triad and its link to ICT is part of the core knowledge required.

Question 4 (b)

(b) Identify **three** risks to Ryan of the hacker having access to their online bank account.

1 .....

2 .....

3 .....

[3]

Most candidates gained at least one mark with many achieving two. Often candidates would give the same answer, phrased in a different way as a different response which unfortunately did not get them an additional mark.

Question 5 (a)

Ryan has confirmed their account was hacked.

The hacker has broken the Computer Misuse Act 1990 when accessing Ryan's online bank account.

5
(a) Explain why the hacker can be prosecuted under this Act.

.....

.....

.....

.....

.....

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

There was a wide degree of understanding of the Computer Misuse Act (CMA) demonstrated by candidates. Candidates who gave the sentences that an attacker could be given did not achieve any marks. Many candidates repeated the question without expanding on it or linking it to any of the crimes under the CMA. The highest scoring candidates identified a provision of the CMA and then expanded this with an explanation of how the hacker's actions broke it.

Question 5 (b) (i)

(b)
(i) Identify **one other** Act that has been broken when the hacker accessed the online bank account.

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

Most candidates achieved this mark.

Question 5 (b) (ii)

(ii) How has this Act been broken?

.....

.....

.....

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

There was a large amount of repetition from question 5 (a) with descriptions of what the hacker had done. There were a limited number of candidates who recognised that it is the company that is prosecuted under the Data Protection Act and therefore their response needed to be written about the bank's shortcomings and not the actions of the hacker.

Question 6 (a)

6

(a) The following table shows cyber security access control methods and their descriptions.

Complete the table by filling in the missing methods and descriptions.

Method	Description
Biometric Access	
	Applying an update to software to close a security vulnerability
Firewall	
Backup	
	Physically connect a computer to a desk to prevent theft

[5]

Some of the identifications and descriptions were well done - biometric access and how to physically prevent theft. However, the use of the word update in the description of the second part should have been a clue that the answer was not update – which many answered with. The descriptions for firewalls and backup were too vague to credit.

Misconception

A patch fixes bugs in the software. An update adds new functionality.

Question 6 (b)

(b) Identify **one** method that will keep the account data safe when in transit and describe how it keeps the data safe.

Method .....

How it keeps the data safe .....

.....

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

Most candidates gained the identification mark on this question and a reasonable number then gave a good description of how it keeps data safe. Where candidates did not achieve full marks for encryption, they focussed on being "unable to read" the data due to encryption rather than "not being able to understand" the data due to it being scrambled.

Misconception

When data has been encrypted it can still be read. It does not make sense which makes it meaningless, but it can be read – putting it cannot be read is incorrect and does not get any marks.

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 exam paper builder platform for a range of our qualifications. Find out more.

Free for all OCR centres with an Interchange account, it allows unlimited users per centre. We require an Interchange username to verify your centre's users for ExamBuilder.

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

Once you have an Interchange username, use the form on this page to sign up for ExamBuilder, or ask an existing user at your centre to create an ExamBuilder account for you.

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 the link to the **Online courses** under the **Assessment** or **Training** tab – hover over **Assessment** or **Training** on the horizontal menu and select **Online courses** from the dropdown.

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?

We recommend all teachers complete the module on Online courses – NEA for their subject. These courses provide subject-specific information about course content; how to prepare for planning, marking and submitting; and support with understanding the marking criteria.

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.

Tell us what you think

Your feedback plays an important role in how we develop, market, support and resource qualifications now and into the future. We want you and your students to enjoy and get the best out of our qualifications and resources, but to do that we need your honest opinions to tell us whether we're on the right track or not.

You can email your thoughts to resources.feedback@ocr.org.uk or visit our feedback page to learn more about how you can help us improve our resources.

Designing and testing in collaboration with you and your students

Helping young people develop an ethical view of the world

Equality, diversity, inclusion and belonging (EDIB) are part of everything we do

---

Contact the team at:

01223 553998

ocr.org.uk

To stay up to date with all the relevant news about our qualifications, register for email updates at ocr.org.uk/updates

Visit our Online Support Centre at support.ocr.org.uk

CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT