OCR
Oxford Cambridge and RSA

Level 3 Alternative Academic Qualification Cambridge Advanced Nationals in Cyber Security and Networks

H037/H137 Unit F193: Fundamentals of cyber security

Sample Assessment Material (SAM)

Time allowed: 1 hour 15 minutes

INSERT required

Please write clearly in black ink. **Do not write in the barcodes.**

Centre number	□□□□□	Candidate number	□□□□
First name(s)			
Last name			
Date of birth	D D M M Y Y Y Y		

INSTRUCTIONS

- Use black ink.
- Write your answer to each question in the space provided. You can use extra paper if you need to, but you must clearly show your candidate number, the centre number and the question numbers.
- In the live exam there might be lined pages at the end of the question paper for you to use if you need extra space. Remember, you must clearly show the question numbers.
- Answer **all** the questions.

INFORMATION

- The total mark for this paper is **60**
- The marks for each question are shown in brackets **[ ]**.
- This document consists of **16** pages.

ADVICE

- Read each question carefully before you start your answer.

Version 1.0 (April 2025)

1 Lavender Haze is a business selling specialist chocolate. The business has two small shops, one in Manchester and one in Leeds. Lavender Haze also has an e-store which can be accessed through their website. The e-store allows customers from all over the United Kingdom to order specialist chocolate and hot chocolate powders.
Each shop stocks a variety of specialist chocolate and uses a shared database of products, which is stored on the business' own server in the Leeds shop. This server, located in a small office, also stores customer information, including names, addresses, food allergies, chocolate preference, phone numbers, email addresses, and credit card details. Lavender Haze stores their staff records on the same server.

(a) The CIA triad is an important concept in cyber security. The C refers to confidentiality.

What do the I and A refer to?

I..

A ....

[2]

(b) Which of the following is **not** confidential customer information stored on the server in the Leeds shop?
Tick (✓) **one** box.

Chocolate preference □

Credit card details □

Email addresses □

Food allergy □

[1]

2 What is the process of only allowing permitted files and applications on a system?
Tick (✓) **one** box.

Biometrics □

Cryptography □

Machine Learning □

Whitelist □

[1]

3 One of the staff has discovered that the server in the Leeds shop has been hacked.

(a) What can hacking also be called?

.... **[1]**

(b) State **two** characteristics of a black hat hacker.

1 ....

2 ....

[2]

(c) Explain **one** possible motivation for a hacker when hacking a business server.

....

....

....

.... **[2]**

4 Following the hack to the server, the manager of the Leeds shop called a cyber security company. The company sent a cyber security analyst and computer forensic engineer to the shop.

Describe **two** responsibilities of a cyber security analyst.

1...

....

....

....

2...

....

....

....

[4]

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

5 Following the visit from the computer forensic engineer the cyber security company provided an incident report to the shop manager in Leeds. The incident report is in the **Insert**.

(a)

(i) Identify the vulnerability vector attacked by the hacker from the incident report.

.... **[1]**

(ii) Explain how the vulnerability vector identified in **5(a)(i)** was attacked.

....

....

....

.... **[2]**

(b)

(i) Identify the incident category level faced by Lavender Haze.

.... **[1]**

(ii) Identify **two** external stakeholders from the incident report that need to be notified of the cyber security incident.

1 ....

2 ....

[2]

(iii) Identify **one** impact in the incident report.

.... **[1]**

(c)
(i) Identify **one** type of information from the incident report that could have been targeted in the cyber security incident on Lavender Haze.

.... **[1]**

(ii) Explain **one** reason why the type of information identified in **5(c)(i)** could have been targeted in the cyber security incident on Lavender Haze.

....

....

....

.... **[2]**

(d) Describe **one** form of disruption that Lavender Haze would have faced due to the cyber security incident.

....

....

....

.... **[2]**

6 As news of the data breach spreads, customers start contacting the shop, worried about their personal information. Some customers report unusual charges on their credit cards and other customers are concerned about identity theft.

Discuss how far you agree with this statement:
Lavender Haze could suffer significant losses because of the cyber security incident.

In your answer you **must** write about:

- the ways you agree with the statement.
- the ways you do **not** agree with the statement.
- **how far overall** you agree **and** your reasons. **[9]**

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

7 The e-store and website are hosted by an external company which Lavender Haze pay a subscription for. Each shop has a fibre connection providing fast internet access. The Leeds shop also has its own unsecured Wi-Fi network linking the shop's computer and till to the business server and website.

The cyber security company identified that the Wi-Fi in the Leeds shop is another weakness that could be attacked.

Explain **one** way that Lavender Haze's Wi-Fi at the Leeds shop could be attacked.

....

....

....

.... **[2]**

8 The cyber security incident report discovered that Lavender Haze did not have adequate security measures in place to prevent the cyberattack. The cyber security company provided several recommendations that should be implemented to reduce the cyber threat faced by Lavender Haze.

(a) Explain **one** way a firewall can protect servers.

....

....

....

.... **[2]**

(b)

(i) Putting a lock on the office door is a physical control that a shop can implement.

Explain how putting a lock on the office door would improve the security of a shop.

....

....

....

.... **[2]**

(ii) State **one** physical control a shop could use, **other than** putting a lock on the office door.

.... **[1]**

9 Customers can purchase chocolate by visiting one of the shops or through the e-store. When customers want to make a purchase through the e-store they must create an account which is stored on the hosted web server. Customers can email Lavender Haze to ask if they have products in stock and place orders.

(a)

(i) State **one** method of protecting data in transit.

.... **[1]**

(ii) Explain how the method stated in **9(a)(i)** protects the data in transit.

....

....

....

.... **[2]**

(b) Outline what a honeypot is.

....

.... **[1]**

(c) Describe **two** advantages of a business using Identity and Access controls.

1..

....

....

....

2..

....

....

....

[4]

Turn over

10 Explain the role of a penetration tester.

....

.... **[1]**

11 One of the other recommendations made by the cyber security company was that Lavender Haze should invest in staff training.

(a) Analyse how increased staff training would improve the security levels for Lavender Haze.

....

....

....

....

....

....

....

....

....

....

....

.... **[6]**

(b) Explain **two** actions that Lavender Haze must do to comply with the Data Protection Act (DPA), **other than** staff training.

1..

....

....

....

2..

....

....

....

[4]

END OF QUESTION PAPER

This is sample assessment material for our specification. It is to help show how the live assessment materials will look. During the lifetime of the qualification, you might see small adjustments to the assessment materials. This is part of continuous improvement, designed to help you and your students. We recommend you look at the most recent set of past papers where available.

OCR
Oxford Cambridge and RSA

Level 3 Alternative Academic Qualification Cambridge Advanced Nationals in Cyber Security and Networks

Unit F193: Fundamentals of cyber security

Sample Assessment Material (SAM)

Mark scheme

This document has **16** pages.

Marking instructions

Crossed-out answers

If a student has crossed out an answer and written a clear alternative, do **not** mark the crossed-out answer.

If a student has crossed out an answer and **not** written a clear alternative, give the student the benefit of the doubt and mark the crossed-out answer if it's readable.

Multiple choice question answers

When a multiple choice question has only one correct answer and a student has written two or more answers (even if one of these answers is correct), you should **not** award a mark.

When a student writes more than one answer

1. Questions that ask for a set number (including 1) of short answers or points

If a question asks for a set number of short answers or points (e.g. **two** reasons for something), mark only the **first set number** of answers/points.

First mark the answers/points against any printed numbers on the answer lines, marking the **first** answer/point written against each printed number. **Then**, if students have not followed the printed numbers, mark the answers/points from left to right on each line and **then** line by line until the set number of answers/points have been marked. Do **not** mark the remaining answers/points.

2. Questions that ask for a single developed answer

If a student has written two or more answers to a question that only requires a single (developed) answer, and has **not** crossed out unintended answers, mark only the first answer.

3. Contradictory answers in points-based questions

When a student has written contradictory answers, do **not** award any marks, even if one of the answers is correct.

Levels of Response marking

1. To determine the level start at the highest level and work down until you reach the level that best describes the answer

2. To determine the mark within the level, consider the following:

Quality of the answer	**Award mark**
Consistently meets the criteria for this level	At the top of the level (6 and 9 mark questions)
Meets the criteria but with some inconsistency	At the middle of the level (9 mark questions)
On the borderline of this level and the one below	At the bottom of the level (6 and 9 mark questions)

ANNOTATIONS

Annotation	Meaning

MARK SCHEME

MARK SCHEME

1 (a)	
Max mark	2 (PO1)
Answer	Two from: • Integrity (1) • Availability (1)
Guidance	1 mark for each correct answer.

1 (b)	
Max mark	1 (PO2)
Answer	• Chocolate preference (1)
Guidance	Correct answer only.

2	
Max mark	1 (PO1)
Answer	• Whitelist (1)
Guidance	Correct answer only.

3 (a)	
Max mark	1 (PO1)
Answer	• Unauthorised access (1)
Guidance	Correct answer only.

3 (b)	
Max mark	2 (PO1)
Answer	**Two** from: • Can be disruptive (1) • Can be destructive (1) • Malicious intent (1) • Patient (1) • Insensitive to consequences (1) • Determined (1) • Risk-taker (1) • Introverted (1) • Unethical behaviour (1) **Credit any other appropriate response**
Guidance	1 mark for each correct answer Question refers to black hat hacker – not grey hat or white hat.

3 (c)	
Max mark	2 (PO1)
Answer	Up to **two** marks for the explanation: **One** mark for stating motivation **One** mark for explaining motivation, e.g.: • Financial gain by accessing the business' bank (1) and stealing from the business' bank account (1) • Identity theft by stealing customer payment details (1) that can be used elsewhere to make payments for goods (1) • Revenge by a past employee who is not happy (1) so they hack in to steal data/disrupt the business (1) **Credit any other appropriate response**
Guidance	Up to **two** marks for each valid motivation identified. Maximum **one** motivation.

4	
Max mark	4 (PO1)
Answer	Up to **two** marks for each responsibility e.g.: **One** mark for stating a responsibility of a cyber security analyst **One** mark for describing the responsibility e.g.: • To defend an organisations system from various online threats (1) by identifying potential security threats and their causes (1) • To monitor the security systems of an organisation using various tools (1) to detect any potential threats or security breaches (1) • To develop recovery plans in case an incident occurs (1) to help an organisation get back up and running following an incident (1) • To develop and implement security policies and procedures to protect the organisation's digital assets (1). They work closely with other departments to ensure personnel apply the policies and procedures (1). **Credit any other appropriate response**
Guidance	Up to **two** marks for each valid responsibility identified. Maximum **two** responsibilities.

5 (a) (i)	
Max mark	1 (PO2)
Answer	Email (1)
Guidance	Correct answer only.

5 (a) (ii)	
Max mark	2 (PO2)
Answer	Up to **two** marks for explanation: **One** mark for identifying how attack took place **One** mark for expansion of how data was accessed e.g.: • Customers' email had a malware file attached (1) that installed itself and ran on the server (1) • Email attachment contained an .exe file (1) that installed and sent data by email to a recipient email account (1) **Credit any other appropriate response**
Guidance	Up to **two** marks for the valid vulnerability vector identified. Maximum **one** vulnerability vector.

5 (b) (i)	
Max mark	1 (PO2)
Answer	• Critical (1)
Guidance	Correct answer only.

5 (b) (ii)	
Max mark	2 (PO2)
Answer	**Two** from: • ICO (1) • Business customers (1) • Legal team (1)
Guidance	These are the only possible answers from the scenario. Do **not** accept: • examples not related to the scenario

5 (b) (iii)	
Max mark	1 (PO2)
Answer	**One** from: • Server only sector attacked (1) • Customer contact details breached (1) • Business stock and supply levels breached (1)
Guidance	These are the only possible answers from the scenario Do **not** accept: • examples not related to the scenario

5 (c) (i)	
Max mark	1 (PO2)
Answer	**One** from e.g.: • Business (1) • Financial (1) • Personal (1)
Guidance	These are the only the responses available from the scenario. Do **not** accept: • examples not related to the scenario

5 (c) (ii)	
Max mark	2 (PO2)
Answer	Up to **two** marks for the explanation e.g.: **One** mark for identifying a reason why the type of information could have been targeted in the incident **One** mark for explaining the reason e.g.: Business e.g.: • To gain data about the Lavender Haze (1) to use against them in a takeover bid (1) • To release the data about stock levels (1) so that Lavender Haze's reputation can be harmed (1) Financial e.g.: • To gain access to Lavender Haze's bank details (1) in an attempt to then steal money from them (1) • To cause the business harm by releasing their financial details (1) so that people can see how successful Lavender Haze is (1) Personal e.g.: • To steal the personal data of customers (1) so that it can be used to carry out other criminal actions (1) • To release the personal data of customers (1) and cause issues for Lavender Haze's reputation (1) **Credit any other appropriate response**
Guidance	Answer must link to the information type identified in part 5**ci.** Up to **two** marks for the valid reason identified. Maximum **one** reason.

5 (d)	
Max mark	2 (PO2)
Answer	Up to **two** marks for describing a disruption **One** mark for identified form of disruption **One** mark for describing how Lavender Haze is affected e.g.: • Lavender Haze would suffer operational disruption as the server is shut down (1). This would prevent any communication by email with suppliers and customers (1). • Lavender Haze would not be able to perform to their normal service levels due to data being accessed/server being shut down (1). This would prevent them fulfilling orders or checking on stock levels (1). • Lavender Haze would suffer financial disruption because they would lose money (1). They would not be able to access and fulfil any email orders/queries from the e-store (1). **Credit any other appropriate response**
Guidance	Up to **two** marks for the valid disruption identified. Maximum **one** form of disruption.

6	
Max mark	9 (PO3)
Levels of Response	**Level 3 (high) 7-9 marks** A **thorough** discussion which shows **detailed** evaluation, which includes: • a **range** of points from **both** sides of the argument • a **detailed** analysis in the context of the question • a **clear** conclusion(s) with **detailed** reasons/justifications • **consistent** use of appropriate subject terminology. **Level 2 (mid) 4-6 marks** An **adequate** discussion which shows **sound** evaluation, which includes: • **some** points from **both** sides of the argument • **some** analysis in the context of the question • an **adequate** conclusion(s) with **relevant** reasons/justifications • **some** use of appropriate subject terminology. **Level 1 (low) 1-3 marks** A **basic** discussion which shows **limited** evaluation, which includes: • a **few** points from the argument • a **limited** analysis in the context of the question • a **brief** conclusion(s) with **limited** reasons/justifications • use of appropriate subject terminology is **limited**. **0 marks** Answer is **not** worthy of credit.
Indicative Content	Answers can include some of the following: Data availability • Disrupted business as data needed for sales is not available to Lavender Haze which means they cannot process sales until completely resolved which can cause losses • May not be a big issue if the data is unavailable for a short period of time Reputation/Customer confidence • Will leave Lavender Haze because they do not trust the company with their data which will reduce the business income • As they found the breach in progress then the number of customers affected might be small, so other customers not affected might remain with the business. • Resolving the issue quickly could enhance the business' reputation. Financial • Significant fine could be levied at Lavender Haze for the release of customer details.

	• There might be minimal loss of money if the situation is resolved quickly so the business can get back up and running. **Credit other relevant conclusions, points and examples.**

7	
Max mark	2 (PO2)
Answer	Up to **two** marks for explaining how the Wi-Fi could be attacked **One** mark for one way Lavender Haze's Wi-Fi could be attacked **One** mark for explanation of the way the Wi-Fi could be attacked e.g.: • Unsecured Wi-Fi network in the shop could be joined (1) and malware could be installed onto server (1) • An unsecured fake access point could be set up using another device (1) so that a customer logs into the fake access point and provides their real Lavender Haze details (1) **Credit any other appropriate response**
Guidance	Up to **two** marks for the valid way Lavender Haze's Wi-Fi could be attacked. Maximum **one** way Lavender Haze's Wi-Fi could be attacked.

8 (a)	
Max mark	2 (PO1)
Answer	Up to **two** marks for explaining how a firewall can protect servers and computers **One** mark for an appropriate way that a firewall can protect servers and computers **One** mark for explanation of the way a firewall protects servers and computers e.g.: • Will monitor attempt to access servers (1) so that attempts to send malware into the system will be flagged/stopped (1) • Emails and other communications from networks will be monitored (1). If there are any abnormal communications from the servers these will be stopped so that nothing is released (1) **Credit any other appropriate response**
Guidance	Up to **two** marks for the valid way a firewall can protect servers. Maximum **one** way a firewall can protect servers.

8 (b) (i)	
Max mark	2 (PO1)
Answer	Up to **two** marks for explaining how putting a lock on the door would improve the security of the office e.g.: • Putting a lock on the door will reduce access to the office (1) as only staff members will have a key so the public cannot just walk in (1) **Credit any other appropriate response**
Guidance	Up to **two** marks for the valid way putting a lock on the door would improve security.

8 (b) (ii)	
Max mark	1 (PO1)
Answer	**One** from e.g.: • Alarm (1) • Swipe card (1) • Biometric (1) **Credit any other appropriate response**
Guidance	Question does not require theft to be stopped – it's just about what could be implemented so there are a wide range of possible controls. Do **not** accept: • Lock on the office door

9 (a) (i)	
Max mark	1 (PO1)
Answer	• Encryption (1) • Two-factor authentication (1)
Guidance	

9 (a) (ii)	
Max mark	2 (PO1)
Answer	Up to **two** marks for explanation e.g.: **One** mark for how the method protects data in transit **One** mark for explaining how the method protects the data in transit e.g.: • (Encryption) the data is converted into meaningless data whilst in transit (1) so that the personal data of the customers cannot be used if the data is hacked (1) • (Two-factor authentication) only allows authorised persons to access the data (1) so when using the system people must sign in using account names/passwords to gain access (1) **Credit any other appropriate response**
Guidance	Answer must link to the information type from part **9ai.** Up to **two** marks for the valid way the method protects data in transit. Maximum **one** way the method protects data in transit.

9 (b)	
Max mark	1 (PO1)
Answer	**One** mark for outlining what a honeypot is e.g.: • Decoy systems set up to entice an attacker (1) • Systems designed to look attractive to an attacker so that the attackers' methods can be captured/monitored/learned from (1)
Guidance	

9 (c)	
Max mark	4 (PO1)
Answer	Up to **two** marks for each advantage: **One** mark for identifying the advantage. **One** mark for describing the advantage, e.g.: • Access to the computer system/data can be tracked so that if there is an issue the business can check who accessed the data last (1). This will allow them to trace the issue back to source (1) • Reduces the chances of data loss for the business (1) as only trusted users/staff can access the system and data (1) • Security is improved as members of the public will not be able to access the computer system (1) as they do not have the rights granted to them by the business (1) **Credit any other appropriate response**
Guidance	Up to **two** marks for each valid advantage identified. Maximum **two** advantages.

10	
Max mark	1 (PO1)
Answer	**One** mark for an explanation of a penetration tester e.g.: • To try and compromise an existing computer system so that any vulnerabilities in the system can be found (1) • Conducting vulnerability assessments of computer systems and networks by simulating cyberattacks to report security flaws (1) • Identifying and analysing security risks and threats to computer systems/ networks/applications through simulating cyberattacks (1) **Credit any other appropriate response**
Guidance	

11 (a)	
Max mark	6 (PO3)
Levels of Response	**Level 3 (high) 5-6 marks** A **thorough** analysis, which includes: • identification of a **range** of characteristics or elements • **detailed** knowledge and understanding in the context of the question • **clear** explanation • **consistent** use of appropriate subject terminology. **Level 2 (mid) 3-4 marks** An **adequate** analysis, which includes: • identification of **some** characteristics or elements • **sound** knowledge and understanding in the context of the question • **adequate** explanation • **some** use of appropriate subject terminology **Level 1 (low) 1-2 marks** A **basic** analysis, which includes: • identification of **at least one** characteristic or element • **limited** knowledge and understanding in the context of the question • **basic** explanation • use of appropriate subject terminology is **limited**. **0 marks** Answer is **not** worthy of credit.
Indicative Content	Answers can include some of the following: Impact of staff training: • How Lavender Haze process customer data when taking orders from emails - ensures that data is stored safely reducing the chance of it being accessed without permission. • How Lavender Haze use/access emails safely so that no malware is installed on the system - how to check emails/attachments to ensure that no malware is included so there is less chance of malware being installed on the system. • How Lavender Haze can monitor computer system use to ensure that staff in the two shops use the system appropriately, to identify if anything outside of normal processes is taking place so that data is not being leaked/sent to somewhere else.

	• How staff answer and reply to emails correctly so that confidential data is not released in attachments. • By ensuring that the staff are aware of Lavender Haze's policies and procedures for dealing with email/customer enquiries. **Credit other relevant analysis, points and examples.**

11 (b)	
Max mark	4 (PO2)
Answer	Up to **two** marks for each action **One** mark for identifying the action. **One** mark for explaining the action, e.g.: • Lavender Haze must not ask for irrelevant data from the customer (1). They must only ask for the data relevant to the purchase and delivery of chocolate when taking an order online (1). • Lavender Haze must only keep customer data whilst it is needed with an active account (1) so they must delete all customer details if they cancel their online account (1). • All the staff data for Lavender Haze employees needs to be stored securely by using a range of security methods (1) to prevent unauthorised access to the data by actors who do not have rights to access the data (1). **Credit any other appropriate response**
Guidance	Up to **two** marks for each valid benefit identified. Maximum **two** benefits. Do **not** accept: • Staff training

Level 3 Alternative Academic Qualification Cambridge Advanced Nationals in Cyber Security and Networks

F193: Fundamentals of cyber security

Sample Assessment Material (SAM)

INSERT

INSTRUCTIONS

- Use this Insert to answer **question 5**.
- Do not send this Insert for marking. Keep it in the centre or recycle it.

INFORMATION

- This Insert contains the incident report.

ADVICE

- Read this Insert carefully before you start your answers.

Cyber Security Incident Report

Date of Notification:
3 June 2025

Incident Location:
Lavender Haze, Leeds

Incident Detector Information

Name:
Casey Taylor

Date and Time Detected:
2 June 2025

8.32am

Title/Job:
Shop Assistant

Location:
Retail outlet – Leeds

Contact Info:
Leeds@LavdrHaze.co.uk

System or Application:
System - Server

Incident Summary

Initial Notification Summary:

- When opening the store for business on 2 June, a member of staff (shop assistant) noticed that the server was running with details appearing on the monitor screen.
- The details were a series of outgoing emails containing customer information and data from the shop till.
- The server is used to store the businesses stock and financial records.
- The business also uses it as an email server.
- The shop assistant notified the shop manager.

Incident Category:

☒ Critical

□ Significant

□ Minor

□ Negligible

Type of Incident:

□ Accidental
☒ Deliberate

Type of Attacker:

□ Internal
☒ External

Incident Notification - Further

Stakeholders requiring possible notification:

☒ Business Owner
☒ Business Administration
□ Business IT Department
□ Human Resources
☒ Information Commissioner Office (ICO)
☒ Business Customer(s)
□ Public Relations
☒ Legal Team
□ System or Application Vendor
□ Other

If ‘Other’ please specify:

Actions

Identification measures:
System logs were checked – indicated the installation of a .exe file received with a customer’s email on 30 May.

Impact of Incident:

- Server only sector attacked.
- Customer contact details breached.
- Business stock and supply levels breached.

Containment Measures:
Server was immediately shut down by shop assistant.

Evidence Collected:
System logs