T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 2

Assignment Brief

Paper number: P002590
v1.0 Summer 2025
24 March 2025 to 28 March 2025
603/6901/2

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA)

Cyber Security

Assignment Brief

Assignment 2

Contents

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider over one week. The times and dates will be specified by NCFE.

The assignment will be completed under supervised conditions.

You must complete all tasks in this assignment independently. You are required to sign a declaration of authenticity to confirm that the work is your own. This is to ensure authenticity and to prevent potential malpractice and maladministration. If any evidence was found not to be your own work, it could impact your overall grade.

Internet access is allowed for tasks 1 and 2.

Ensure all print screens have been labelled with a brief description of what is being shown.

Save your work regularly as you work through the assessment.

Students must submit the work as stated in the evidence requirements and in-line with file naming conventions.

Electronic files should be named using the following format for identification purposes – Surname_Initial_student number_evidence reference, for example: Smith_J_123456789_Task1_investigation report.pdf.

Timing

You have 10 hours to complete all tasks within this assignment. Each task has the following number of hours:

Task 1 = 7 hours 30 minutes (this will be completed in two sessions)

Task 2 = 2 hours 30 minutes (this will be completed in one session)

Individual tasks must be completed within the timescales stated for each task, but it is up to you how long you spend on each part of the task, therefore be careful to manage your time appropriately.

Marks available

Task 1 = 42 marks

Task 2 = 18 marks

Details on the marks available are provided in each task.

You should attempt to complete all of the tasks.

Read the instructions provided carefully.

Performance outcomes (POs)

Marks will be awarded against the skills and knowledge performance outcomes (POs) as follows:

Task 1

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data [24 marks]

PO2: Propose remediation advice for a security risk assessment [18 marks]

[42 marks]

Task 2

PO3: Discover, evaluate and apply reliable sources of knowledge [18 marks]

[18 marks]

Scenario

Hawker Tech Solutions UK is a growing organisation selling assistive technology solutions and consultancy services to small- or medium-sized enterprises (SMEs). Following a recent cyber security attack it is looking to improve all aspects of its network security and to modernise its enterprise network.

Cecilia works in the payroll department at Hawker Tech Solutions UK and has a reported a number of issues.

She finds her computer frustrating to use, with it running slow when she has several applications open. She receives personal and client emails that often contain attachments. She regularly opens the attachments and confirms they have been received. Cecilia is now concerned there is an issue with her computer which she is unable to resolve.

Cecilia works in the office full time, 5 days a week.

The IT manager has not noticed any issues with the main system but is aware of the problems Cecilia has been having. The IT manager would like to ensure these issues are resolved and do not pose a threat to the wider business network.

Task 1: investigate and take corrective action

Time limit

7 hours and 30 minutes.

You can use the time how you want, but all parts of the task must be completed within the time limit.

[42 marks]

Brief

Cecilia has provided you with access to her computer. She has described the problems she is experiencing when using it as follows:

- her computer is often unresponsive and is frustrating to use
- programs are regularly freezing and not responding
- some files are not opening.

You are required to research what may be causing these issues.

You will then need to investigate and assess any vulnerabilities that may exist by analysing the emails and identifying any issues and possible resolutions.

You will be required to identify actions that could be taken to resolve the issues.

Instructions for students

Part A

In relation to this brief, firstly you must create a report that:

- discusses how these issues could be the result of either a cyber attack or an internal software program problem – you should clearly identify how you would differentiate between the two
- explains how and why the issues could have occurred
- identifies the types of attack it could be

Part B

You have full administration rights and access to Cecilia's computer (this will be a virtual machine assigned to you by your tutor). Using the virtual machine (VM), you must:

- log into the machine using the following credentials:
  - **username:** Cecilia
  - **password:** Password1
- investigate the emails and assess any potential issues that may exist
- run a scan using an online virus checking tool (for example, VirusTotal) to identify what attack, if any, has taken place

In your report, you should:

- record your findings (this should include screenshots to evidence your investigation and use of the scan)
- suggest potential fixes for any issues that are identified

Part C

In your report, you should:

- provide an outline of any remedial actions that could be implemented to better protect the current system (for example, any additional security methods that could be used), including any future recommendations

Resources

For this task, you will have access to the following:

- word processor
- internet access
- VM (provided by tutor)

Evidence required for submission to NCFE

The following evidence should be submitted:

- report document including evidence from parts A, B and C, in PDF format

Task 2: ongoing maintenance

Time limit

2 hours 30 minutes.

You can use the time how you want, but all parts of the task must be completed within the time limit.

[18 marks]

Brief

Following the resolution of the issues identified in task 1, you have been requested to produce a report that evaluates how ongoing maintenance will ensure the network and systems remain secure and effectively operational.

Instructions for students

Create an evaluative report that:

- recommends ongoing maintenance measures that could be implemented to ensure the system remains secure and operational – this should ensure that the issues encountered in task 1 do not occur again in the future
- recommends any remedial action you would take to ensure these measures are implemented, and justifies the approach taken
- identifies the additional requirements to ensure these measures are manageable
- explores any systems upgrades that might be required based on these measures

Resources

For this task, you will have access to the following:

- word processor
- internet access

Evidence required for submission to NCFE

The following evidence should be submitted:

- a written evaluative report, in PDF format

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

NCFE is authorised by the Institute for Apprenticeships and Technical Education to develop and deliver this Technical Qualification.

Owner: Head of Assessment Solutions.