T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

All assignments

Provider Guide

Paper numbers: P002589, P002590, P002591
v1.0
Summer 2025
603/6901/2

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

Cyber Security

Provider Guide

All assignments

Past Paper

Contents

About this document

This guidance has been produced in order to support with the delivery of the T Level in Digital Support Services occupational specialism (OS) in Cyber Security. The Provider Guide is not intended to replace the other assessment materials and supporting documents but should be used in conjunction with them.

This document addresses all assessments for the Cyber Security OS.

Introduction

The aim of these assessments is to allow students the opportunity to demonstrate the knowledge and skills they have gained on the Cyber Security OS. The assessment methods vary to allow students to express their knowledge and skills in a valid and reliable way and for them to be able to demonstrate threshold competency.

NCFE provides instructions for each of the assessments and providers should follow them. Providers **must** purchase essential resources prior to the assessments taking place. A full equipment list can be found in the Qualification Specification.

Past Paper

General information

The OS assessments are a set of synoptic assessments that are externally set and externally marked.

The term ‘synoptic assessment’ refers to the combination of the three assignments in this OS component.

The term ‘assessment’ is used in the same way as ‘assignment’ but will often refer to specific properties of the assignment.

Accessibility and fairness

To promote accessibility and fairness for all students and to ensure diversity and equality, we expect providers to be aware of and meet the requirements of relevant NCFE policies and government legislation. You must ensure that:

- all of your processes concerned with assessment are carried out in a fair and objective manner
- you continue to adhere to current equal opportunities legislation
- you continue to operate an effective Diversity and Equality Policy, with which students are familiar and which applies to all students using NCFE’s products and services

Plagiarism

Plagiarism may result in the external assessment task being awarded a U grade.

For further guidance refer to the plagiarism in external assessment and the suspected malpractice policies and procedures located on the NCFE website.

Access arrangements

Access arrangements enable students with special educational needs, disabilities, or temporary injuries to take NCFE examinations and assessments. Any of the listed tasks may be adapted to suit different needs, but the way in which they are adapted depends on the individual need or disability.

It is important that any adaptation or adjustment does not compromise the rigour and validity of the assessment; in most cases extra time (which should be applied for) or a change of recording mode (for example, changing to handwritten submissions) are appropriate modifications.

NCFE can make arrangements for students with disabilities and those with special educational needs to help them access the assessments, as long as the competences being tested are not changed. Access arrangements must be agreed with NCFE before the assessment by using our online application service. All access requests will be considered individually, and your application should outline what the student can do and how the activities will be adapted in order to meet the assessment criteria.

Adapted activities will not be accepted for assessment unless approved by NCFE.

Malpractice / maladministration

Students **must not** share any details of the assessment, their progress, or their evidence with peers, either within or outside their setting, at any time during or after the assessment when within the specified assessment windows. Provider staff should regularly remind their students about potential repercussions of breaches of security by referring to the NCFE guidance and regulations available on the website.

If at any time during an assessment there is a violation of these regulations, the designated person has the right to stop the assessment immediately; this decision must only be made in exceptional circumstances where malpractice is irrefutable. Once stopped, no allowance can be given retrospectively if the decision is deemed invalid.

If malpractice occurs during an assessment, providers should inform NCFE immediately with a report of what occurred – please read suspected malpractice policies and procedures available on the NCFE website.

If any of the regulations are breached by a student or other persons, involved in the conduct of the assessment, then NCFE may declare the assessment void.

In the event of a suspected or actual breach of these regulations by students:

- the work completed by the students concerned and any unauthorised materials (if applicable) must be confiscated from the students and given to the relevant persons as noted in the guidance and regulations document
- all students suspected of breaching these regulations should be instructed to leave the supervised assessment environment immediately, if appropriate to do so, causing the least amount of disruption to other students
- NCFE should be informed immediately of any irregularity via a phone call or email
- the provider should conduct its own investigation into the incident and report the incident and their findings to us using the NCFE notification of malpractice document on the NCFE website

NCFE reserves the right to investigate each case of alleged or actual malpractice / maladministration committed by a student, provider or other persons involved in the conduct of the assessment in order to establish all of the facts and circumstances surrounding the case. The investigation will be carried out in accordance with NCFE's suspected malpractice policies and procedures.

Past Paper

About this assessment

The Cyber Security occupational specialism (OS) is assessed synoptically with a suite of three assignments. The assignments require the student to independently apply an appropriate selection of knowledge, understanding, skills and techniques developed throughout the full course of study, in response to briefs and / or tasks. This will allow the student to demonstrate that they have met a level of threshold competence across the performance outcomes (POs) of the OS.

The assessment methods vary across the assignments to allow students to demonstrate the knowledge and skills they have acquired throughout their learning and experience.

The assessments validly and reliably allow the student to be able to demonstrate, at the end of the qualification, the threshold competency gained in order to progress into employment or into higher education.

NCFE provides instructions for each of the assessments, and these must be followed by T Level providers.

Essential resources for each assessment, where applicable, must be purchased by the provider prior to the assessments taking place. The resources required for each assessment will be taken from the exemplar / broader range of resource requirements outlined in the Qualification Specification; however, attention should be given to any particular resource-specific requirement within this document.

The synoptic assessment for this OS is graded pass, merit or distinction, and the final grade will contribute 50% of the overall technical qualification grade, so it is important that students have the opportunity to produce work of the highest standard they can. The assignments within this synoptic assessment are designed to allow the student to do this in a way that is as occupationally authentic to the roles that they may take on in future employment.

Past Paper

What is threshold competence?

‘Threshold competence’ is defined as a level of competence that:

- signifies that a student is well placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the technical qualification in a college-based setting, with a substantial industry placement
- signifies that a student has achieved the level for a pass in relation to the relevant OS component

What is synoptic assessment?

A synoptic assessment is a form of assessment in which students are required to demonstrate that they can identify and use, in an integrated way, an appropriate selection of skills, techniques, concepts, theories, and knowledge from across the technical area, relevant to the tasks.

Synoptic assessment is integral to high quality technical qualifications to allow students to demonstrate a holistic understanding of the sector, making effective connections between different aspects of the subject content.

The assignments and tasks in this assessment are designed to be synoptic in a way that is as occupationally realistic as possible.

What will students be assessed on?

Students will be assessed against the following set of performance outcomes (POs) that describe what the student should be able to do:

Cyber Security POs	
PO1	Apply procedures and controls to maintain the digital security of an organisation and its data
PO2	Propose remediation advice for a security risk assessment
PO3	Discover, evaluate and apply reliable sources of knowledge

Assessment structure

The following synoptic assessment, comprised of three assignments, has been designed to test to what extent a student can meet the skills and underpinning knowledge required to achieve threshold competence for Cyber Security.

The occupational specialism (OS) will comprise of the following assessments, which will assess the knowledge and skills gained from the occupational specialist component:

	Sub-component	Assessment time	% weighting	Raw marks	Assessment conditions	Marking
Occupational specialism (OS)	Assignment 1: project proposal and set-up devices, network and access.	11 hours	20%	50	Supervised	External
	Assignment 2: practical skills assessment following processes and procedures.	10 hours	40%	60	Supervised	External
	Assignment 3: practical skills assessment, troubleshooting and a written task.	6 hours 30 minutes	40%	70	Supervised	External
	Component total	**27 hours 30 minutes**	**100%**	**180**		

Past paper

The guidance below explains the nature of this assessment and should be used alongside the general guidance provided in this document, the Qualification Specification, and live assessment materials (once available).

The synoptic assessment consists of three assignments covering the following areas:

1. Project proposal and set-up devices, network and access in response to a brief.
2. Practical skills assessment following processes and procedures.
3. Practical skills assessment, troubleshooting and a written task.

Assignments are broken down into tasks where necessary. The assignments, tasks, and further guidance (within this document) are to support tutors, and show how the assignments are expected to be delivered.

Evidence produced by students for the assignments will be sent to NCFE for marking. Assessment judgements, including overall judgement of the performance required at each of the grade boundaries, will be made by NCFE and results released to the provider at the appropriate time.

This assessment consists of:

- assignment 1: project proposal and set-up devices, network and access in response to a brief (11 hours)
  - task 1: 5 hours 30 minutes
  - task 2: 5 hours 30 minutes
- assignment 2: practical skills assessment following processes and procedures (10 hours)
  - task 1: 7 hours 30 minutes
  - task 2: 2 hours 30 minutes
- assignment 3: practical skills assessment, trouble shooting and a written task (6 hours and 30 minutes)
  - task 1: 2 hours 30 minutes
  - task 2: 2 hours
  - task 3: 2 hours

This synoptic assessment must be completed for a student to achieve the T Level Technical Qualification in Digital Support Services with the Cyber Security OS.

Assignments 1, 2 and 3 are designed to assess a student's knowledge, understanding, and skills in an occupationally authentic and practical context across the performance outcomes (POs) of this technical qualification (TQ), and contribute to the student's overall grade.

Past Paper

Assessment timings

Assessment delivery guidance can be found for each assignment in the assignment and task-specific guidance section.

Assessment windows and dates

Assignment 1 will be available as a dated assessment, as per the Key Dates Schedule on the NCFE website. All students must sit the assignment on this date at the same time. Assignment 1 is externally assessed. Evidence for assignment 1 must be returned to NCFE for marking after completion.

Assignment 2 will be available to the provider as an assessment sat during a window, as per the Key Dates Schedule on the NCFE website. Assignment 2 is externally assessed. Evidence for assignment 2 must be returned to NCFE for marking after completion.

Assignment 3 will be available as a dated assessment, as per the Key Dates Schedule on the NCFE website. All students must sit the assignment on this date at the same time. Assignment 3 is externally assessed. Evidence for assignment 3 must be returned to NCFE for marking after completion.

A submission deadline for the evidence for assignments 1 to 3 will be set for each academic year to allow NCFE to carry out remote moderation before the release of results in August of that year.

All evidence created, generated and recorded for these assignments is subject to data protection rules and information should be anonymised to protect the rights of individuals where relevant.

All assignments are **unseen**. All assessment materials or knowledge of any assessment materials should not be provided to the student until the specified day and start time of each assessment.

Past Paper

Assessment conditions

The Cyber Security OS consists of three separate assignments.

The assignments are set by NCFE and administered by you, the provider, and externally marked by NCFE examiners (unless stated otherwise).

The assignments will be released to providers for planning, preparation and set up only, in advance of the windows and not for teaching and learning purposes, or to be given to the students to prepare:

- assignment 1 will be delivered within week 1 of a set assessment window, on the dates and times specified by NCFE:
  - this assessment is externally marked
  - evidence for assignment 1 must be returned to NCFE for marking after completion
- assignment 2 will be delivered within weeks 2 and 3 of a set assessment window, specified by NCFE, to take place after the assessment window for assignment 1:
  - this assessment is externally marked
- assignment 3 will be delivered within week 4 of a set assessment window, specified by NCFE, to take place after the assessment window for assignment 2:
  - this assessment is externally marked
  - evidence for assignment 3 must be returned to NCFE for marking after completion

Assessment conditions guidance can be found for each assignment in the assignment and task-specific guidance section.

Students must complete the OS assessments independently and under supervised conditions, as per the guidance within the assignment and task-specific instructions section.

Students and tutors are required to sign one External Assessment Cover Sheet (EACS) declaration of authenticity form to confirm that the work is their / the student's own. A single form is sufficient for all tasks within each assignment. The declaration forms can be located on the NCFE website. This is to ensure authenticity and to prevent potential malpractice and maladministration. Students must be made aware of the importance of this

declaration and the impact this could have on their overall grade if the evidence was found not to be the student's own work. Tutors **must** be aware that by signing the declaration, they are validating it is the student's own work.

Where appropriate, tutors **must** retain students' research materials at the end of each supervised session, alongside all materials and / or evidence produced by students within the supervised assessment.

At the end of each supervised session, the tutor **must** collect all evidence and any other materials, including students' research materials, before students leave the room, to ensure that no student takes **any** external assessment material or assessment evidence out of the room. This also includes sufficient monitoring and checks to ensure that students have not made materials available to themselves or anyone else electronically via the intranet or internet.

Students will be asked not to share the details of the assessment with peers at their own or with other providers. Inevitably there may be some advantage to students who take the assessment at the end of the assessment window, but this is considered to be minimal given the narrow window. Staff and students will be regularly reminded about potential repercussions of breaches of security, as per the NCFE Regulations for the Conduct of External Assessment.

External assessment materials should be securely stored between supervised sessions. Students must not have access to this area between the supervised sessions, including electronic files.

Work such as formative assessment and / or work done with sample assessment materials must not be used again as part of the external assessment task submission to NCFE.

Students are not allowed to bring **any** prepared materials into the supervised sessions unless otherwise stated in the assessment-specific instructions. This **must** be monitored by providers.

Appendices should not be included and will not be marked unless specifically required from the task instructions.

Students are not allowed access to any online cloud storage or email and chat services during the assessment, this should be monitored by the providers.

NCFE recognises that some providers deliver to very large cohorts, in such cases staff and physical resources will similarly have been scaled up during teaching and learning to cope with a large cohort. On balance, we consider this option to be both sensible in terms of security of assessment and manageable for providers.

Digitally produced work, such as audio recordings, need to be securely stored using a file naming convention framework, including provider name, provider number, student name, student number, assignment number and task number.

Past Paper

Controls for this assessment

Assessment delivery

The Cyber Security occupational specialism (OS) consists of three separate assignments.

The assignments are set by NCFE and administered by you, the provider.

The assignments will be released to providers for planning and preparation in advance of the windows:

- assignment 1 will be delivered on set times and dates across all providers
- assignment 2 will be delivered within a set 1-week window specified by NCFE after the set dates for assignment 1

- assignment 3 will be delivered on set dates and times across all providers after the window for assignment 2.

Specific information for each assignment can be found below.

Students must complete the assignments independently and under supervised conditions, as per the specific guidance for each assignment provided below.

Students and tutors are required to sign a declaration of authenticity for each assignment to confirm that the work is their / the student's own. A single declaration form is sufficient for all tasks within one assignment. The declaration forms can be found on the NCFE website. This is to ensure authenticity and to prevent potential malpractice and maladministration. Students must be made aware of the importance of this declaration and the impact this could have on their overall grade if the evidence was found not to be the student's own work. Tutors **must** be aware that by signing the declaration, they are validating it is the student's own work.

At the end of each supervised session, the tutor **must** collect all evidence and any other materials before students leave the room, to ensure that no student takes any external assessment material or assessment evidence out of the room. This also includes sufficient monitoring and checks to ensure that students have not made materials available to themselves or anyone else electronically via the intranet or internet.

External assessment materials should be securely stored between supervised sessions. Students must not have access to this area between the supervised sessions, including electronic files and physical hardware.

Resources and equipment

The resources required for each assessment will be available in the specific guidance for each assignment in this document. These requirements will be in line with the resources specified in the Qualification Specification and as such, students should be familiar with these as they should be used during the delivery of the qualification.

Past Paper

Assignment 1

Controls

The tasks for this assignment will be delivered over 2 days, on the dates and times specified by NCFE.

Task 1 will be administered on day 1.

Task 2 will be administered on day 2.

Students have 11 hours to complete all tasks within this assignment.

Task 1 = 5 hours 30 minutes (this will be completed in one session on day 1)

Task 2 = 5 hours 30 minutes (this will be completed in one session on day 2)

Students must work independently and under supervised conditions.

Students should be given a separate user account that is locked at the end of each assessment session.

Internet access is allowed for task 1 and task 2.

All screenshots should be labelled and included in the submitted evidence.

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

Evidence should be returned to NCFE by the date specified and will be marked by NCFE.

Note: where internet access is not available providers will provide an alternative solution for the installation of software.

Past Paper

Resources

Providers need to ensure that students have access to the following resources:

Task 1

- internet access
- word processing software

Task 2

- internet access
- word processing software
- device with no operating system (OS) installed (this may be a laptop / computer / virtual machine (VM))
- an OS for students to install (for example, Windows 10)
- software for installation:
  - anti-malware solution (for example, Windows Defender, MalwareBytes, Comodo Internet Security Free)
  - back-up solution (for example, File History, ToDo Backup Free, Veeam)
  - full disk encryption software (for example, BitLocker, VeraCrypt, DiskCryptor)

Note: a provider could give the students a copy of the software for the installation or direct them to a suitable website to download. For the purposes of task 2, the provider may choose an appropriate vendor and version for the students to install. The software provided by the provider does not need to be the same as that identified by the students in task 1. Where internet access is not available, a USB storage device / external drive may be used for the supply and installation of software to allow this task to be completed.

Past Paper

Assignment 2

Controls

The assignment will be delivered within a set one-week window, specified by NCFE.

Students have 10 hours to complete all tasks within this assignment.

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

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

For task 1, providers **must** schedule two sessions lasting 3 hours 45 minutes, to ensure that all students complete all tasks by the end of the window. Task 1 sessions can be scheduled across 2 days.

For task 2, providers **must** schedule one session lasting for 2 hours 30 minutes, to ensure that all students complete all tasks by the end of the window.

Students must work independently and under supervised conditions.

Students should be given a separate user account that is locked at the end of each assessment session.

Internet access is allowed for task 1 and task 2.

All screenshots should be labelled and included in the submitted evidence.

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

Evidence should be returned to NCFE by the date specified and will be marked by NCFE.

Past Paper

Resources

Providers **must** ensure that students have access to the following resources:

Task 1

- internet access
- word processing software
- NCFE supplied virtual machine (VM)

Task 2

- internet access
- word processing software

Virtual machine (VM)

The VMs are made available to all providers and should be downloaded and tested prior to the start of the assessment window to ensure there are no issues. This will offer a standardised approach to assessment and ensure that no students are disadvantaged. These VMs have been created using VirtualBox and exported as an Open Virtualization Format (OVF) file. This VM contains a Linux Operating System (OS), email client and three vulnerable emails.

Test environment

Task 1 will be carried out using the NCFE-supplied VM.

Note: if the recommended online scanning software (VirusTotal) is unavailable students can choose any other online virus scanning software or providers may provide a recommended link for them to use.

Security issues

Emails

Messages for task 1 are saved in the .eml format, this format is text-based and easily readable by Thunderbird, which is installed on the VM. These are three different examples of how to either infect a device through an infected attachment or steal information though a fake email.

Past Paper

Assignment 3

Controls

The tasks for this assignment will be delivered over 2 days, on the dates and times specified by NCFE.

Tasks 1 and 2 will be administered on day 1.

Task 3 will be administered on day 2.

Students have 6 hours 30 minutes to complete all tasks within this assignment, including 30 minutes to read through the additional supporting document ('Company Overview - Assignment Brief Insert').

Task 1 = 2 hours 30 minutes (this will be completed in one session on day 1).

Task 2 = 2 hours (this will be provided after completion of task 1 and be completed in one session on day 1).

Task 3 = 2 hours (this will be provided after completion of task 2 and be completed in one session on day 2).

Students must work independently and under supervised conditions.

Students should be given a separate user account that is locked at the end of each assessment session.

Internet access is allowed for task 1, task 2 and task 3.

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

Evidence should be returned to NCFE by the date specified and will be marked by NCFE.

Past Paper

Resources

Providers **must** ensure that students have access to the following resources:

Task 1

- word processing software
- risk assessment template (more lines can be added as required)
- internet access

Task 2

- word processing software
- internet access

Task 3

- word processing software
- internet access

Risk assessment template (assignment 3 task 1)

Threat (identification of possible threat to the network)	**Vulnerability** (vulnerability related to threat identified)	**Asset** (assets at risk)	**Impact** (impact if threat is exploited)	**Likelihood** (likelihood that threat is exploited)	**Risk** (overall risk to business)	**Action** (recommended action)	**Control type** (type of control implemented as mitigation)

Risk levels: low | medium | high | critical	**Business control types:** physical | administrative | technical	**Mitigating control types:** preventative | detective | corrective | deterrent | directive | compensating | acceptance

Past Paper

Document information

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2025.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

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.

Past Paper