T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

All assignments

Provider guide

v1.1: Specimen assessment materials
21 November 2023
603/6901/2

Internal reference: DSS-0013-08

NCFE

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

Cyber Security

Provider guide

All assignments

Contents

Controls for this assessment

Assessment delivery

The Cyber Security occupational specialism consists of 3 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.

Assignment 1

Controls

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

Students have 11 hours to complete all tasks within this assignment

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

Task 2 = 5 hours 30 minutes (this will be completed in 1 session in 1 day)

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 print screens should be labelled and included in the .pdf file.

Students must submit the work as a single .pdf file at the end of the assessment.

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

Resources

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

- internet
- word processing software
- laptop/computer/virtual machine
- firewall software/virtual private network (VPN) software/anti-virus software

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 stick/external drive may be used for the supply and installation of software to allow this task to be completed

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 2 sessions)

Task 2 = 2 hours 30 minutes (to be completed in 1 session)

For task 1, providers must schedule 2 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 1 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 2.

Students must use an electronic .pdf file to record all evidence against each task.

All print screens should be clearly labelled and linked to or included with the relevant task.

Students must submit their work as a single .pdf file at the end of the assessment.

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

Resources

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

Task 1

- word processing software
- supplied virtual machine (VM)

If students are unable to evidence the scanning process through screenshots the tutor will be able to provide a witness testimony to record observation of the task.

Task 2

- word processing software

Virtual machine

NCFE has worked in conjunction with Cisco Network Academy to give access to the virtual machines for all providers to use. This will offer a standardised approach to assessment and give a level field for all students, which will ensure no students are disadvantaged.

Cisco Network Academy virtual machines 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. These virtual machines have been created using Virtual Box and contain a Linux OS, email client, 3 vulnerable emails and links to the online scanning software.

Test environment

Task 1 will be carried out using the supplied virtual machine

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. There are 3 different examples of how to either infect a device through an infected attachment or steal information though a fake input form.

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. Internet access is allowed.

Task 3 will be administered on day 2. Internet access is allowed.

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’).

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 1 session on day 1)

Task 3 = 2 hours (this will be provided after completion of task 2 and be completed in 1 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.

Students must submit the work as a single .pdf file at the end of the assessment.

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

Resources

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

- word processing software
- the internet
- risk assessment template (task 1) - see appendix 1

Appendix 1

Risk assessment template (assignment 3 task 1)

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
Such as passwords cracked by attacker	Lack of password complexity policy	Files or data on file shares High	Critical data could be accessed by a malicious attacker and stolen Critical	Attackers would need access to the network or password hash to attempt this Medium	Data is exfiltrated from the company with potential to damage company reputation, breach of GDPR with financial implications and potential for customers becoming victims of identity theft High	Implement complex password policy in directory services	Technical/ preventative
							(further lines can be added as required)

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

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication		01 June 2023
v1.1	Sample added as watermark	November 2023	21 November 2023