T Level Technical Qualification in Digital Support Services

Employer set project (ESP)

Core skills

Cyber Security

Provider guide

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

Internal reference: DSS-0001-02

T Level Technical Qualification in Digital Support Services
Employer set project (ESP)

Core skills

Provider guide

Cyber security

Contents

About this document

Document security

Please do not distribute this document to students. This is for provider and tutor use only. All tutors must be familiar with the information in this document. This document should be kept secure at all times.

This document should be read along with the regulations for conduct of external assessment. Assessment conditions and resources are defined in the qualification specific instructions for delivery (QSID). These documents can be found on the NCFE website.

About the employer set project

The purpose of the employer set project is to ensure that students have the opportunity to apply core knowledge and skills to develop a substantial piece of work in response to an employer set brief. The brief and tasks are contextualised around an occupational area and chosen by the student ahead of the assessment window.

To achieve the assessment objectives and meet the brief, students must demonstrate the following core skills (CS):

CS1: Communicate information clearly to technical and non-technical stakeholders.

CS2: Working with stakeholders to clarify and consider options to meet requirements.

CS3: Apply a logical approach to solving problems, identifying and resolving faults, whilst recording progress and solutions to meet requirements.

CS4: Ensure activity avoids risks to security.

The knowledge requirements will be taken from the core knowledge relevant to the brief and the briefs will change for each assessment window.

Administering the external assessment

The maximum overall time allowed for the external assessment is 12 hours 10 minutes under supervised conditions. The individual timings for each task are detailed later in the document. The table below shows when providers may run each task and at which stage of the assessment window each task should be completed by:

Task	Issuing of assessment materials	Week 1	Week 2
1	Issue the ‘Project brief – Task 1’ document, including control documents A, B and C.	NCFE fixed date: Monday	-
2	In addition to the above, issue the ‘Project brief – Task 2’ document.	Tuesday to Friday	-
3	In addition to the above, issue the ‘Project brief – Task 3’ document, including control document D.	-	NCFE fixed date: Monday
4	In addition to the above, issue the ‘Project brief – Task 4’ document.	-	Tuesday to Friday

NCFE sets the start date and the submission date of the assessment window for the external assessment task. External assessment material should not be given to students until the first supervised assessment session.

The assessment window will consist of provider-arranged supervised sessions of external assessment. Sessions can be undertaken in the normal classroom environment, so long as each student has access to, or the option to use, a computer system. Providers can decide how to arrange supervised sessions for tasks 2 and 4. Tasks 1 and 3 are set on fixed dates and times set by NCFE. Providers must submit students' completed assessment work by the published submission date.

When preparing to start a supervised session, time taken to print students' work is not included as part of the permitted hours for the external assessment task. In addition to this, time taken to collate and upload students' work is also not included as part of the permitted hours for the external assessment time.

Control documents A, B, C and D should be provided to students at the appropriate time throughout the assessment. Further instructions are detailed in the task specific instructions, in this document, and the control documents are available in the relevant project brief documents.

Control documents A, B and C are part of Project brief – Task 1

Control document D is part of Project brief – Task 3.

At any time, NCFE may request the timetable that providers have set for the supervised sessions.

The permitted time must not be increased unless a reasonable adjustment has been agreed for a student in accordance with the access arrangements and reasonable adjustments policy and special considerations policy, which can be found on the NCFE website.

The permitted time must not be decreased. Students must be given the opportunity to complete the full amount of time for the external assessment task. Providers must take this into account when timetabling the sessions.

In the event the student misses a supervised session the following procedure must be followed.

If a student misses a fixed-date session (task 1 or 3) providers must not re-arrange another time for the student to complete the session. They must follow the reasonable adjustments and special considerations policy, which can be found on the NCFE website.

If a student misses a session that does not have a fixed date, providers may rearrange a suitable time for the student (providing it is in the appropriate assessment window). However, task 2 must be completed by all students before moving on to task 3.

Each student is allowed up to a maximum of 15 minutes rest break during the tasks which have 3 or more hours allocated (tasks 3 and 4) and breaks must be managed by the provider. These breaks must be in a supervised, controlled room and monitored by the provider.

Marking the external assessment task

The external assessment tasks are set and marked by NCFE. This means that providers must not assess, internally quality assure or provide any feedback to the student about their performance in the external assessment task. However, tutors may be asked within a specific task to validate and generate supplementary evidence of student performance. The supervised external assessment tasks must be treated independently of the teaching of the outline content.

Instructions for tutors

Assessment conditions

Students must complete the employer set project independently and under supervised conditions, as per the specific guidance for each task later in the document.

Students are required to sign an external assessment cover sheet (EACS) and a declaration of authenticity form to confirm that the work is their own. A single form is sufficient for the whole project. 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 retain all materials and/or evidence produced by students within the supervised assessment at the end of each supervised session.

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, for example, via the 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.

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.

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.

Plagiarism

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

For further guidance, refer to the student handbook – plagiarism guidance and maladministration and malpractice guidance, which is located on the NCFE website.

Resources

Students must have access to the appropriate resources required to complete the employer set project. These include the following:

- access to the internet (though this should be limited to ensure that access to online cloud storage services and/or online chat clients is not accessible)
- privacy mode should be disabled on any web browser and policies applied to prevent deletion of browsing history
- appropriate word processing and spreadsheet software

Internet access

This project is designed to simulate a real-world task the student may be given in the workplace. Internet access is appropriate for completion of this project as the student would be able to research error messages and potential solutions in a real-world setting. The assignment has been structured to test students' ability to complete real-world tasks and internet access will not compromise this. Internet access is allowed throughout all tasks, though the use of online cloud storage or chat services should be restricted to ensure that students do not share materials or access any prior work completed before the assessment.

This list is not exhaustive, and you need to refer to the qualification specification for subject-specific details.

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 our products and services

Assessment and task specific instructions

The employer set project briefs

For each assessment window, there will be 3 versions of the employer set project available for booking; each version is contextualised against the occupational specialisms relevant to the pathway. These 3 briefs will be set by employers in conjunction with NCFE and will be different for each assessment window.

The briefs are designed to ensure a motivating starting point for students and will be based on a real-world problem.

Selection of brief

Students are required to discuss and agree with their tutor which of the following occupational-based briefs they would like to take forward for their employer set project:

- Digital Infrastructure and Network Cabling
- Digital Support
- Cyber Security

The provider must book students onto the appropriate version of the employer set project by the deadline for that specific assessment series as indicated on the key dates schedule, which can be found on the NCFE website.

Bookings will be made on the NCFE portal, and guidance can be found in the portal handbook which can be accessed within the system.

Delivery guidance

Task 1

- task 1 will take place on a fixed date set by NCFE within the assessment window
- the student should be issued control documents A, B and C for this task, which are available in the project brief
- the student should be allowed access to the internet to allow them to research and identify solutions to the problem
- the student should prepare and submit a fault-finding investigation report and a test plan document

Task 2

- students must be supervised from the start of this task until all parts of the task are complete
- students should be allowed access to the internet if they wish to research anything to help them construct their set of interview questions
- students will be working independently, planning their information gathering for this project – as part of this they will need to interview the operations and IT manager:
    - the operations and IT manager interview should be conducted as a recorded role play with the provider supplying someone with appropriate technical knowledge to play the role of the operations and IT manager (it is recommended that 1 person is provided per 10 students – this is to facilitate completion of the interviews in a timely manner):
        - it is acceptable that the tutor can play this role or someone with appropriate technical understanding; however, the person conducting the interview responses must be informed using only the interviewer's notes
    - the specific interviewer guidance to support providers with the completion of task 2 is detailed at the end of this document – Operations and IT manager notes (interviewer's notes to support task 2)

Task 2 should be delivered to all students within the provider, on a specific day within the assessment window. Providers should plan how they are going to administer the task, and this will vary depending on the size of the cohort and staff availability. It may be appropriate to give each individual student different start times which are staggered (with enough time to allow for setting up the audio recording equipment). The following table is not intended to be prescriptive but should serve as a guide of how providers may stagger the start times of students to effectively administer the task.

Task 2: start time	Task 2: interview start time	Task 2: task complete time	Student
9:00am	10:00am	11:10am	A
9:15am	10:15am	11:25am	B
9:30am	10:30am	11:40am	C
9:45am	10:45am	11:55am	D

- task 2 can begin at different times for students; however, once students have completed their interview they must go to a controlled, supervised room
- task 2 can be completed over more than one day; however, all students must complete task 2 within the first week of the assessment window
- students will have 1 hour to prepare their questions for the interview which will then be carried out 1 hour after the start
- interviews should last no longer than 10 minutes
- once the interview is complete, the student will have the remaining 1 hour to complete the task
- in answering questions, tutors should refer to the Operations and IT manager's notes (interviewer's notes to support task 2), which are detailed at the end of this document
- where a student asks questions outside the brief, the operations and IT manager should explain they do not have the answer to that question at this time
- the brief document should not be provided to the student
- the operations and IT manager interviews must be completed in a private space, with the role play submission being recorded as an audio file
- the tutor must ensure the interview is recorded in the correct format and will be responsible for uploading the recording for the student
- task 3 must not commence until all students have completed task 2 to prevent them accidentally seeing or receiving information before it is appropriate; providers must therefore ensure that all interviews have taken place before the fixed scheduled date of task 3
- email templates will be provided for this task, students should not use their own email accounts to construct the 2 emails required as evidence for the task

Task 3

- task 3 will take place on a fixed date set by NCFE within the assessment window
- providers must ensure that students are given a copy of the specification of requirements (control document D) at the start of the task – this can be found in the Project brief – Task 3 document
- students will be required to submit a detailed security management project proposal which includes a detailed network topology network diagram
- it is appropriate that students have internet access to allow them to research and develop an effective solution to the scenario

- each student is allowed up to a maximum of 15 minutes rest break during this task; breaks must be supervised by the provider

Task 4

- students should be allowed access to the internet
- students should be allowed access to all previous employer set project materials, apart from the interview audio recording
- students are required to submit a sample satisfaction survey document and a post-project review document
- each student is allowed up to a maximum of 15 minutes rest break during this task, breaks must be supervised by the provider

Timings

The timings below have been devised to support student and provider planning:

Task 1 = 2 hours 30 minutes

Task 2 = 2 hours 10 minutes

Task 3 = 4 hours

Task 4 = 3 hours 30 minutes

Total = 12 hours 10 minutes

Instructions for completing and submitting the external assessment tasks

The external assessment tasks must be completed and uploaded at the end of each session.

Once task 2 has been completed, students' work from task 1 and 2 should be stored securely to prevent information distributed for task 3 being used to amend the first 2 tasks.

Tutors are encouraged to ensure that students follow the filename conventions specified in the external assessment tasks for each individual document, which is Surname_Initial_student number_evidence reference, for example: Smith_J_123456789_Task1.

Where evidence reference is shown, this should be replaced with the task number for which the work reflects. All files must be saved in .pdf format. These files, per student, should be placed within a single folder before being zipped and submitted.

Students must respond to each task individually and follow the document structure when submitting their evidence as per the evidence requirements section within each task. They must not combine responses for separate tasks.

Operations and IT manager's notes (interviewer's notes to support task 2)

Instructions

Please refer to these notes when conducting the recorded network manager interview as part of task 2.

This interview should be conducted as a role play and recorded as part of the assignment submission. Where questions are asked that are wider than the brief of this document, it is appropriate to give relevant responses to allow the student to gather all information they wish.

Information should not be offered unprompted, but student questions should be given complete answers.

Network setup

Network, servers and firewalls

Currently, Willow Technology maintains 2 servers located in a dedicated server room based at its head office in Winchester – one is to provide file and print services, the other is to add redundancy into the system. These servers were configured when the company started and have worked successfully for the last 2 years so have not been updated as to not affect performance.

The current company network security policies have been in use for a long time and have not yet been updated to meet the growing size of the company. Whatever the outcome of this project, the business plans to install new servers and firewall. The company also plans to update its user permissions in the next 12 months.

Server specifications:

Server 1: File and Print Services

Server name: DC01

Operating system: Windows Server 2008R2

Roles:

- file services
- print services
- domain name system (DNS)
- dynamic host configuration protocol (DHCP) – 30 users

Server 2: Redundant Server

Server name: FS01

Operating system: Windows Server 2008

Roles: Redundancy

Previously, no remote access facilities were provided because there was no demand for remote working. A third server has recently been set up to support this. This new virtual private network (VPN) server has been set up at short notice and is running on a spare desktop PC from the office.

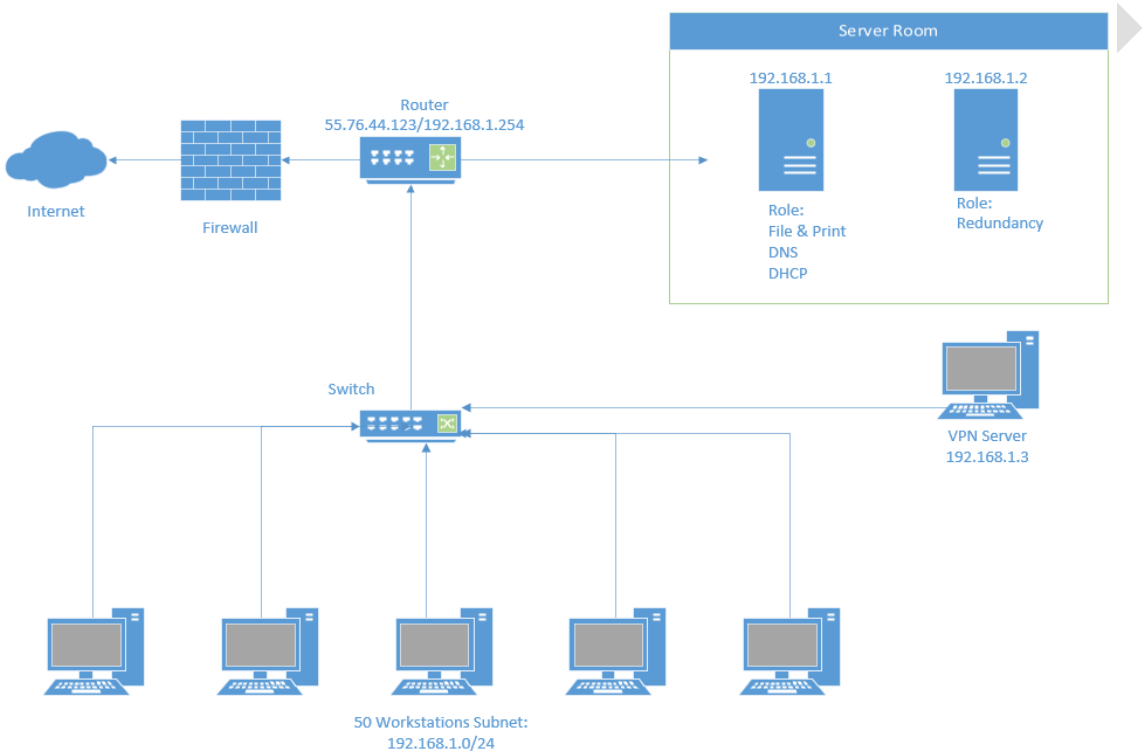
Server 3: VPN Server

Server name: RAS01

Operating system: Windows Server 2019

Roles: VPN access

Network topology



Client PCs

Willow Technology has a workforce of 50 employees.

Staff working in the office use desktop workstations provided for them. However, as the company allows remote working, staff can work from home.

All client PCs are configured with anti-malware software (2019 edition). Scheduled updates to the operating system are on a quarterly basis, updates to anti-malware are monthly and updates to application are not scheduled but reviewed on request.

Currently, all users have the same level of access so that all staff can access all resources.

Remote access

Staff working remotely are issued with a work laptop.

Staff induction

A set of videos, totalling 3 hours of training, is provided to staff as part of their induction, which introduces them to the network, software, systems and security. There are no requirements for staff to complete this again as the company feels that after staff have completed their probation, they will be confident in the company system and requirements.

Current firewall policy

This firewall policy is expected to provide security functionality by enforcing intents on traffic that passes through our network devices. Traffic is permitted or denied based on the action defined as the firewall policy intent.

The firewall policy provides the following features:

- by default, all network traffic is permitted with rules in place to deny traffic if issues occur
- permits, rejects, or denies traffic based on the application in use
- future consideration to identify not only hypertext transfer protocol (HTTP) but also any application running on top of it, enabling the company to properly enforce policies – for example, an application firewall intent could block HTTP traffic from Facebook but allow web access to HTTP traffic from Microsoft Outlook

Table 1: The firewall policy protocol rules

Action	Service	Protocol	Source address	Destination address	Port
Allow	HTTP	TCP	192.168.1.0/24	Any	80
Allow	HTTPS	TCP	192.168.1.0/24	Any	443
Allow	POP3	TCP	192.168.1.0/24	Any	110
Allow	SMTP	TCP	192.168.1.0/24	Any	25
Allow	DHCP	UDP	192.168.1.0/24	192.168.1.1	67/68
Deny	SSH	TCP	192.168.1.0/24	Any	22
Deny	FTP	TCP	192.168.1.0/24	Any	21
Deny	SFTP	TCP	192.168.1.0/24	Any	22

Project requirements

The senior management team are very keen to identify ways to use cloud resources to manage company computers. Therefore, assume that the current servers are due to be retired. Any solution you propose should either replace or remove the need to maintain the onsite servers.

Your solution should include:

- a robust solution for storing, managing and providing access to company files and data, regardless of location
- ability to manage company computers and devices centrally
- virtual desktop solution to allow secure access to data on personal equipment
- a solution that will allow staff to communicate and collaborate effectively with each other

Additional tutor interview guidance

- the firewall is currently configured as the policy
- the VPN server is a PC located in the main workplace as a temporary measure
- users all have the same privileges with one user account for all users apart from IT, which has administration rights
- the fake email has been highlighted as the reason behind the ransomware attack
- it is not possible to identify how many staff followed the link in the email, although no one raised the email as a concern
- new staff watch a 3-hour staff training session that covers IT systems, the network and security but this is not monitored, assessed or reported on
- there is currently no additional training for existing staff as the company feel that staff are competent following their probation
- the router is not configured with any additional security, as the firewall controls all the security
- there is currently a system in place to back up data, but this is done at the end of each month using a full back up; this means that the backup data is currently 3 weeks old at the time of the attack

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 a watermark	November 2023	16 November 2023