T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 1

Mark scheme

v1.1: Additional sample material
16 November 2023
603/6901/2

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

Digital Support

Mark scheme

Assignment 1

Contents

Marking guidelines

General guidelines

You must apply the following marking guidelines to all marking undertaken throughout the marking period. This is to ensure fairness to all students, who must receive the same treatment. You must mark the first student in exactly the same way as you mark the last.

The mark scheme must be referred to throughout the marking period and applied consistently. Do not change your approach to marking once you have been standardised.

Reward students positively giving credit for what they have shown, rather than what they might have omitted.

Utilise the whole mark range and always award full marks when the response merits them.

Be prepared to award 0 marks if the student's response has no creditworthy material.

Do not credit irrelevant material that does not answer the question, no matter how impressive the response might be.

The marks awarded for each response should be clearly and legibly recorded.

If you are in any doubt about the application of the mark scheme, you must consult with your team leader or the chief examiner.

Guidelines for using extended response marking grids

Extended response marking grids have been designed to award a student's response holistically for the relevant task or question and should follow a best-fit approach. The grids are broken down into levels, with each level having an associated descriptor indicating the performance at that level. You should determine the level before determining the mark.

Depending on the amount of evidence that the task produces, the grids will either be a single, holistic grid that covers the range of relevant performance outcomes (POs), and will require you to make a judgement across all the evidence, or they will consist of multiple grids that will be targeted at specific POs, and will require you to make a judgement across all the evidence in relation to that particular grid in each case, therefore making multiple judgements for a single task to arrive at a final set of marks. Where there are multiple grids for a particular task, it is important that you consider all the evidence against each of the grids, as although the grids will focus on particular POs, awardable evidence for each grid may come from across the range of evidence the student has produced for the task.

When determining a level, you should look at the overall quality of the response and reward students positively, rather than focussing on small omissions. If the response covers aspects at different levels, you should use a best-fit approach at this stage and use the available marks within the level to credit the response appropriately.

When determining a mark, your decision should be based on the quality of the response in relation to the descriptors. Standardisation materials, marked by the chief examiner, will help you with determining a mark. You will be able to use exemplar student responses to compare to live responses, to decide if it is the same, better or worse.

To support your judgement, the indicative content is structured in such a way that mirrors the order of the different points within the band descriptors. This will allow you to use the 2 in conjunction with each other by providing examples of the types of things to look for in the response, for each descriptor. In other words, the indicative content provides you with a starting point of possible examples and the bands express the range of options

available to you in terms of the quality of the response. You should apply the standards that have been set at relevant standardisation events in a consistent manner.

You are reminded that the indicative content provided under the marking grid is there as a guide, and therefore you must credit any other suitable responses a student may produce. It is not a requirement either that students must cover all of the indicative content to be awarded full marks.

Performance outcomes (POs)

This assessment requires students to:

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

PO2: Install, configure and support software applications and operating systems

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1

(20 marks)

Task 1(a): system preparation

Band	Mark	Descriptor
4	7–8	There are excellent and well-justified recommendations and a detailed understanding of implementing a broad range of business control techniques within the workplace and for remote working (physical and administrative). There is a detailed explanation demonstrating a comprehensive understanding of how to operate the data systems effectively and securely. There is an excellent reference to GDPR/DPA 2018 and evidence of detailed understanding of the legislation and all 7 principles.
3	5–6	There are appropriate recommendations and a good understanding of implementing a range of business control techniques within the workplace and for remote working (physical and administrative). There is a good explanation demonstrating a clear understanding of how to operate the data systems effectively and securely. There is a good reference to GDPR/DPA 2018 and evidence of a good understanding of the legislation and at least 5 of the principles.
2	3–4	There are some suggestions and a limited understanding of implementing some business control techniques within the workplace and for remote working (physical or administrative). There are relevant suggestions of how to operate the data systems effectively or securely. There is some reference to GDPR/DPA 2018 with evidence of some understanding of the legislation and at least 3 of the principles.
1	1–2	There is a vague and very basic understanding of implementing limited business controls within the workplace and for remote working (physical or administrative). There are basic/limited suggestions of how to operate the data systems securely. There is limited reference to GDPR/DPA 2018 with little evidence of understanding and little or no reference to any of the 7 principles.
	0	No creditworthy material.

Indicative content

Task 1(a): system preparation

Recommendations on implementing business control techniques within the workplace could include:

- preventative measures (for example, fencing/gate/cage, separation of duties, 2-step authentication)
- detective measures (for example, CCTV, logs, audit, remote logins, security)

- corrective measures (for example, fire suppression, standard operating procedures – office and remote)
- deterrent measures (for example, security guards, employment contracts, home working policies)
- directive measures (for example, signage, agreement types, general security policies)
- compensating measures (for example, air conditioning, role-based awareness training)
- recovery measures (for example, back-ups, business continuity)
- video conferencing physical security (for example, frosted windows on internal facings, external windows including mirrored finish)

GDPR/DPA 2018 could include references to the 7 principles:

1) Lawfulness, fairness and transparency

2) Purpose limitation

3) Data minimisation

4) Accuracy

5) Storage limitation

6) Integrity and confidentiality (security)

7) Accountability

Note: The above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief

Task 1(b): network planning

Band	Mark	Descriptor
4	10–12	A full health and safety risk assessment has been carried out using a full range of methods, with clearly identified actions to control risks. Remote working has been thoroughly considered as a factor with detailed understanding of the challenges and risks. There is excellent evidence of planning on setting up a network with excellent evidence of timescale planning, a comprehensive inventory and a highly detailed network design including IP addressing schema. An excellent security risk assessment for the work has been undertaken that follows all ISO 27001 principles and clearly identifies mitigations.
3	7–9	A good health and safety risk assessment has been carried out using a wide range of methods with appropriate actions to control risks. Remote working has been well considered as a factor with an understanding of the challenges and risks. There is good evidence of planning on setting up a network with good evidence of timescale planning, a good inventory and detailed network design including IP addressing schema. A good security risk assessment for the work has been undertaken that follows most ISO 27001 principles and identifies most mitigations.

Band	Mark	Descriptor
2	4–6	A satisfactory health and safety risk assessment has been carried out using a limited range of methods with some actions to control risks. Remote working has been considered as a factor with a satisfactory understanding of the challenges and risks. There is some relevant evidence of planning on setting up a network in relation to timescales, inventory and satisfactory network design including IP addressing schema. A relevant security risk assessment for the work has been undertaken that follows some ISO 27001 principles and identifies some mitigations.
1	1–3	A basic health and safety risk assessment has been carried out using few methods with few actions to control risks. There is vague and very basic evidence of planning on setting up a network in relation to timescales, inventory and network design. A very basic security risk assessment for the work has been undertaken that follows few ISO 27001 principles and identifies few mitigations.
	0	No creditworthy material.

Indicative content

Task 1(b): network planning

A health and safety risk assessment that may include health and safety threats, risks and hazards is listed below, but is not limited to:

- policies and standard operating procedures
- lone working
- manual handling/safe lifting
- working at height
- fire safety
- RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013)
- display screens

Actions to control risks may include, but are not limited to:

- redesigning the job
- replacing the materials, machinery or processes
- organising work to reduce exposure to the materials, machinery or process
- identifying and implementing practical measures needed to work safely
- providing personal protective equipment (PPE) and making sure workers wear it

Students are to produce evidence of planning in setting up a network which may include, but is not limited to:

- timescale of network – for each installation, students are to produce a network planning schedule in a suitable format that allows tracking and updating of tasks, identifying the task needing to be done and the timeframe of installation along with suitable commentary for each step
- inventory – specifying the devices and specifications, such as 40 computers in the Midlands office, a switch, 1 server, 2 colour printers, plus the ability to use mobile phones which will be connected to the network; also, all video conferencing devices and specifications – to include secure connections, video and audio facilities
- network design – a detailed design showing all devices connected to the network, as mentioned in the inventory, and showing the connectivity
- class of IPV4 (class A, B or C) IP schema with subnet mask calculations and network ranges allocated – the schema should consider the following:
    - the IP addressing schema would be internal and not an IP address issued by InterNIC/RIPE
    - students should assess the IP network class based upon the number of devices to be accommodated (for example, a class A network can support up to 16,777,214 hosts and a class C network can support up to 254 hosts)
    - students should consider whether 'static' IP addresses are to be allocated and if so by which means, such as static addresses assigned from a manual pool (for example, spreadsheet) or DHCP reservations
    - students in band 4 should demonstrate knowledge of the local loopback address used by a machine to refer to itself – ISO 27001
    - students in band 4 should demonstrate that the 0 address in the range (for example, 192.168.1.0) refers to 'this network' and the 255 address (for example, 192.168.1.255) is used as a broadcast to send a message to all devices
    - students in band 4 will also be able to refer to other network parameters, such as primary and secondary DNS and default gateway

Students are to carry out a security risk assessment (ISO 27001) which should:

- identify risks – including a list that includes, for example, hard copies of information, electronic files, removable media, mobile devices and intangibles (such as intellectual property)
- analyse risks – assign the impact/likelihood values based on risk criteria
- evaluate risks – prioritise which risks need to be addressed in which order:
    - select risk treatment options
    - computer viruses, rogue security software, trojan horses, adware and spyware, DOS and DDOS attacks, phishing, rootkit

Note: The above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief

Task 2

(56 marks)

Task 2(a): install and configure a small-scale network

Criteria/step in the process	Marks	Marking guidance
Evidence of implementing physical network and network security measures	3	Award marks as per the following descriptors: 1 – little evidence of implementing network with limited planning and few screenshots 2 – some evidence with good planning and appropriate screenshots of implementing physical network and network security measures 3 – detailed evidence with comprehensive planning and excellent screenshots of implementing physical network and network security measures
Evidence of installing Windows Server	3	Award marks as per the following descriptors: 1 – limited evidence of installing Windows Server with basic explanation and limited use of correct terminology 2 – some evidence of installing Windows Server with well-explained measures and mostly correct terminology 3 – detailed evidence of installing Windows Server with detailed and well-explained measures and correct terminology
Evidence of creating Active Directory	6	Award marks as per the following descriptors: 1–2 – limited evidence of creating Active Directory with basic explanation and limited use of correct terminology 3–4 – some evidence of creating Active Directory with well-explained measures and mostly correct terminology 5–6 – detailed evidence of creating Active Directory with detailed and well-explained measures and correct terminology
Evidence of setting up necessary user accounts and groups	3	Award marks as per the following descriptors: 1 – limited evidence of setting up user accounts and groups with basic reference to role-based access control 2 – some evidence of setting up user accounts and groups with well-explained reference to role-based access control 3 – detailed evidence of setting up user accounts and groups with excellent reference to role-based access control, explaining why role-based access control is important

Criteria/step in the process	Marks	Marking guidance
Evidence of software licence management	3	Award marks as per the following descriptors: 1 – limited evidence of managing software licences and limited use of correct terminology 2 – some evidence of managing software licences (recorded in a document) with well-explained measures and mostly correct terminology 3 – detailed evidence of managing software licences (recorded in a document) with detailed and well-explained measures and correct terminology
Total marks	**18**	

Task 2(b): install and deploy

Criteria/step in the process	Marks	Marking guidance
Installing an operating system (OS) (for example, Windows)		
Carry out installation and deployment along with the source of the image	6	Award marks as per the following descriptors: 1–2 – little evidence of OS installation with limited time spent configuring and patching and limited use of correct terminology 3–4 – some evidence of OS installation with limited time spent configuring, patching and installing anti-virus software, with mostly correct terminology 5–6 – detailed evidence of OS installation along with remote server access and extensive configuration, patching and anti-virus software, including signature update and using correct terminology
Installing application software suitable for the client		
Install office software (for example, Microsoft Office)	1	Award mark if completed and evidence is provided.
Create guidance explaining how to install a VPN OR Install VPN system	1	Award mark if EITHER have been completed and evidence is provided.
Install instant messaging software/applications (for example, Skype for Business or Microsoft Teams)	1	Award mark if completed and evidence is provided.

Criteria/step in the process	Marks	Marking guidance
Configure email client software (for example, iCloud, Google/Gmail, Exchange Online, Yahoo)	1	Award mark if completed and evidence is provided.
Implementing suitable back-up security controls		
Evidence that back-up procedures have been set up	2	1 mark if back-up procedures completed and evidence is provided. 2 marks if back-up procedures completed and confirmation that they are working as expected.
Installing necessary drivers		
Device manager has no missing driver	1	0 marks if any drivers outdated or missing. 1 mark if 0 drivers missing – all updated.
Setting up and configuring a WiFi mobile device to allow for network connectivity		
Evidence of wireless data network	2	1 mark if connected to WiFi network. 1 mark if connected to WiFi network and evidence it is working as expected.
Configuring a mobile device to include security measures and back-up		
Evidence of implementing screen locks or biometric security measures	1	Award mark if completed and evidence is provided.
Evidence of locator applications (for example, find my mobile)	1	Award mark if completed and evidence is provided.
Configuration of cloud back-up	1	Award mark if completed and evidence is provided.
Carrying out all necessary updates including anti-virus		
Evidence of OS and application updates required	2	1 mark if no pending OS updates. 2 marks if evidence that OS and application updates are all current.
Installing mobile security software	2	1 mark if mobile security software installed. 2 marks if mobile security software installed and evidence provided is up to date.
Total marks	**22**	

Task 2(c): installation notes

Band	Mark	Descriptor
4	13–16	There is excellent knowledge, including detailed, thoughtful comments in the installation notes for the software installation. Installation notes are comprehensive and record all software installations, upgrades, uninstalls and major configuration changes for the workstations and mobile device. The student has identified all vulnerabilities to the current system/network with excellent recommendations. The technical language used is excellent and is highly detailed for the digital support team. There is excellent use of English – spelling, punctuation and grammar.
3	9–12	There is good knowledge, including sufficient comments on the installation notes for the software installations. Installation notes are detailed and record most software installations, upgrades, uninstalls and major configuration changes for the workstations and mobile device. The student has identified most key vulnerabilities to the current system/network with good recommendations. The technical language is good and appropriate for the digital support team. There is good use of English – spelling, punctuation and grammar.
2	5–8	There is some knowledge, including some relevant comments on the installation notes for the software installations. Installation notes are brief and record some software installations, upgrades, uninstalls and major configuration changes for the workstations and mobile device. The student has identified some vulnerabilities to the current system/network with satisfactory recommendations. The technical language is reasonable and mostly appropriate for the digital support team. There is sound use of English – spelling, punctuation and grammar.
1	1–4	There is some basic knowledge, including limited comments on the installation notes for some of the software installation. Installations notes lack detail and record few software installations, upgrades, uninstalls and major configuration changes for the workstations or mobile device. The student has identified limited vulnerabilities to the current system/network with weak recommendations. The technical language used is limited, and occasionally appropriate for the digital support team. There is basic use of English – spelling, punctuation and grammar.
	0	No creditworthy material.

Indicative content

Installation notes for the software installations:

The purpose of the installation notes is to record all software installations, upgrades, uninstalls and major configuration changes for the workstation. The installation log could include:

- computer identification (for example, workstation name/number)
- location (where the workstation is located – for example, HR office)
- details on the installation of the video conferencing system (for example, set-up, location, screen and video layout)
- details of installation (for example, install/uninstall, reinstall and upgrade)
- who it was that carried out the work (name of employee)
- when the work took place (date/time)
- how to install/uninstall the software (for example, step-by-step instructions on how to do this for the OS and application software)
- recommendations for future releases/updates

Identifying vulnerabilities to the current system/network, for example, could include:

- the potential vulnerabilities in critical systems
- user account control
- single point of failure
- mission essential functions
- remote working issues
- open port access:
  - USB
- optical media:
  - CD/DVD, network ports
- wireless networks

Technical language would consist of correct use of key words, for example:

- system
- workstation
- end-user
- application software
- anti-malware
- back-up measures
- application types
- application installation
- peripherals
- upgrades
- installation

- configuration
- vulnerabilities and threats
- impact and risk management
- risk mitigation

Note: The above is not an exhaustive list; credit should be given to other suggestions as appropriate to the scenario in the brief

Performance outcome grid

Task	PO1	PO2	PO3	Total
1(a)	6	1	1	8
1(b)	8	3	1	12
2(a)	4	13	1	18
2(b)	1	20	1	22
2(c)	1	3	12	16
Total marks	20	40	16	76
% weighting	26%	53%	21%	100%

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	Additional sample material		01 September 2023
v1.1	Sample added as a watermark	November 2023	16 November 2023