



T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Network Cabling

Assignment 2

Mark scheme

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

Network Cabling

Mark scheme

Assignment 2

Contents

Marking guidelines	3
Task 1: install the cabling system	5
Task 2: devise a test plan and test the cabling system	9
Performance outcome (PO) grid	13
Document information	14
Change History Record	14

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 bands, with each band having an associated descriptor indicating the performance at that band. You should determine the band 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 band, you should look at the overall quality of the response and reward students positively, rather than focusing on small omissions. If the response covers aspects at different bands, you should use a best-fit approach at this stage and use the available marks within the band 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 and test cabling in line with technical and security requirements

Sample

Task 1: install the cabling system

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

Band	Mark	Descriptor
4	10–12	Excellent application of the principles of network security when configuring network devices. Highly proficient use of appropriate techniques when configuring the WiFi network. At least 2 other security controls are implemented.
3	7–9	Good application of the principles of network security when configuring network devices. Effective use of appropriate techniques when configuring the WiFi network. An additional security control is implemented.
2	4–6	A reasonable attempt at applying principles of network security when configuring network devices but may miss some key factors. Reasonable use of appropriate techniques when configuring the WiFi network, which may not be effective in some cases.
1	1–3	A limited or minimal attempt at applying principles of network security when configuring network devices, missing many key factors. Limited and sometimes ineffective use of appropriate techniques when configuring the WiFi network.
	0	No creditworthy material.

Indicative content

Application of the principles of cyber security for internet-connected devices, systems and networks (confidentiality) will cover configuration of the switch with VLAN functionality, for example, VLAN 1 and VLAN 2.

Tools and techniques (encryption) will be achieved by applying relevant security controls for the WiFi access, for example, WPA2, configuring the router firewall, configuring a VPN and changing the default password.

Principles of network security should be mentioned in the explanation:

- the CIA triad – confidentiality, integrity and availability
- IAAA (identification, authentication, authorisation and accountability)
 - security authentication process

- using passwords and security implications

Tools and techniques (encryption) will be achieved by applying relevant security controls for the network access, for example:

- WPA2
- firewalls
- configuring the router firewall
- configuring a VPN
- changing the default password
- confirming the firmware is up to date
- hiding the SSID of the network

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

PO2: Install and test cabling in line with technical and security requirements

Band	Mark	Descriptor
4	16–20	<p>An excellent cabling system with evidence of exceptional workmanship.</p> <p>Exceptional use of tools, following health and safety where required.</p> <p>Highly effective installation of the cabling system meeting the technical and security requirements of the scenario and with full and accurate labelling of all components.</p>
3	11–15	<p>A good cabling system with evidence of confident workmanship.</p> <p>Proficient use of tools, following health and safety where required.</p> <p>Effective installation of the cabling system meeting technical requirements of the scenario and with accurate labelling of most components.</p>
2	6–10	<p>A reasonable cabling system with evidence of some workmanship or incorrect cable set-up.</p> <p>Satisfactory use of tools, following health and safety where required but may not always be fully proficient.</p> <p>Reasonable installation of the cabling system but may include some faults relating to technical requirements of the scenario and with adequate labelling of some components.</p>
1	1–5	<p>A simplistic cabling system with evidence of limited workmanship.</p> <p>Basic use of tools, following health and safety where required.</p> <p>Poor installation of the cabling system, which may not be in line with most technical requirements of the scenario and with limited or mostly inaccurate labelling of components.</p>
	0	No creditworthy material.

Indicative content

Network installation evidence of meeting technical requirements will include:

- installation and configuration of core network components, with appropriate labelling to facilitate testing, including:
 - completed wall outlet sockets
 - router, switches and wireless access points, plus configured:
 - encryption
 - DHCP

- types and features of connectors that can be applied within network cabling
- the creation of correctly configured cables, to a TIA/EIA 568B standard, installed to produce a working network
- consideration of health and safety to meet the requirements of legislation, regulations and standards such as:
 - Personal Protective Equipment Regulation 2018
 - Work at Height Regulations 2005
 - Health and Safety at Work etc Act 1974
- indicators of quality workmanship and compliance with network cabling working practices:
 - all sheaths grabbed by the RJ45 clamp
 - all cables inserted to the end of the RJ45 connector
 - correct labelling of circuits, cables, and equipment
 - comprehensive testing of all cabling
 - identification of system errors

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: devise a test plan and test the cabling system

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

Band	Mark	Descriptor
4	7–8	<p>Testing of the security controls used to avoid potential vulnerabilities is comprehensive, effective and includes multiple methods.</p> <p>Comprehensive testing evidence has been provided, which covers the complete installation and has fully relevant solutions/recommendations to any issues identified.</p>
3	5–6	<p>Testing of the security controls used to avoid potential vulnerabilities is effective but may only use a single method.</p> <p>Detailed testing evidence has been provided, which covers the complete installation and has relevant solutions/recommendations to any issues identified.</p>
2	3–4	<p>Testing of the security controls used to avoid potential vulnerabilities is carried out with some effectiveness but is missing some information.</p> <p>Reasonable testing evidence has been provided, which covers some aspects of the installation and has solutions/recommendations for some of the issues identified.</p>
1	1–2	<p>Testing of the security controls used to avoid potential vulnerabilities is limited in its effectiveness and is missing key information.</p> <p>Limited testing evidence has been provided, which covers minimal aspects of the installation and has few solutions/recommendations for any issues identified.</p>
	0	No creditworthy material.

Indicative content

Cable tester readings and other forms of digital communication testing, for example, ICMP Ping or traceroute.

Preventative business control techniques to avoid potential vulnerabilities apply to logical security, for example, WiFi access having appropriate security configured such as WPA2 rather than WEP.

Other controls can include firewalls, VPN and password settings.

Physical security measures include making sure network devices are in a secure location, and that cables have been secured throughout, in either trunking or a safe place, like a suspended ceiling.

Tests could include:

- MAC filtering appropriately denies or grants access to network where appropriate

- appropriate level of encryption applied to the wireless connection (router or WAP)
- quality checking appropriate firewall rules (students do not have to demonstrate the rules in use)
- authentication methods working as expected and are reasonably complex
- netsh WLAN show WLAN report from command prompt
- network properties in, for example, Windows or Linux
- network properties on tablets/mobile devices

Solutions and recommendations could include:

- identifying the correct wireless encryption
- ensuring appropriate network security (for example, wireless passwords, MAC filtering)
- identifying incorrect or ineffective firewall rules
- implementing appropriate physical security controls

Testing should be evidenced and where tests fail, an explanation of what steps have been taken to rectify.

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

PO2: Install and test cabling in line with technical and security requirements

Band	Mark	Descriptor
4	4	Comprehensive and highly proficient testing of the cabling system, including more than one test being carried out on multiple components and including test plan documentation that has multiple entries for a range of components. Excellent use of networking test tools.
3	3	Effective but not necessarily comprehensive testing of the cabling system, covering most of the required elements in the system and including test plan documentation that covers the majority of the system but may have missed 1 or 2 elements. Comprehensive use of networking test tools.
2	2	Some testing of the cabling system, showing some skill, but is missing some tests including key components of the system. The test plan documentation is missing required entries. Acceptable use of networking test tools.
1	1	Minimal testing of the cabling system, with test plan documentation provided that may be missing key information and provides minimal insight into the testing process. Limited or ineffective use of networking test tools.
	0	No creditworthy material.

Indicative content

Cable testing, applying appropriate testing tools, in accordance with the manufacturer's equipment procedures and in compliance with TIA/EIA standards. This should be done by using cable tester readings and other forms of digital communication testing, for example:

- ICMP Ping
- traceroute
- ipconfig
- FTP put/get
- Windows and Linux system utilities

Network cabling inspection parameters, for example:

- a visual inspection of a cable has been completed.
- is the cable inserted all the way into the RJ45 connector?
- do the twisted pairs reach the copper connectors inside the RJ45 connector?
- is the RJ45 connector fully clamped onto the twisted pair cable?

Impact of poor workmanship and non-compliance with network cabling practices – are there any cables that do not perform at the maximum speed, or cables that are too long, causing signal degradation?

Cable testing could include:

- end-to-end of cables with cable tester
- port to patch panel with cable tester
- device to device connectivity with appropriate devices (for example, laptop to desktop)
- cables follow correct pin-out to EIA/TIA 568B standards

Component testing could include:

- wireless connectivity
- communication between devices and router (both wired and wirelessly)
- IP address distribution (DHCP)

Solutions and recommendations could include:

- re-terminating wall sockets or patch panel points
- re-terminating RJ45 heads
- replacing faulty cables
- altering configuration of devices
- recommendation of alternative hardware with different or increased functionality

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 (PO) grid

Task	PO1	PO2	PO3	Total
1	12	20		32
2	8	4		12
Total marks	20	24		44
% weighting	45%	55%		100%

Document information

Copyright in this document belongs to, and is used under licence from, the Institute of Apprenticeships and Technical Education, © 2023.

'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.

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.

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

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 watermark	November	16 November 2023