T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Network Cabling

Assignment 3

Mark scheme

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

NCFE

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

Network Cabling

Mark scheme

Assignment 3

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 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 focussing 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

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1: troubleshooting faulty cables

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

Fault	Steps taken by student	Marks
Cable 1: cable has been damaged when it was run throughout the trunking – a new 10m cable needs to be created	Student correctly configures wires for straight-through cable.	1
	Student fits RJ45 the correct way up.	1
	Student correctly crimps RJ45 with outer covering gripped by crimp.	1
	Student tests cable and confirms correct functioning as a straight-through cable.	1
Cable 2: outer sheath of Cat5e has split, starting at the connector and running approximately 10cm down the length of the cable	Student correctly configures wires for straight-through cable.	1
	Student correctly crimps RJ45 with outer covering gripped by crimp.	1
	Student tests cable and confirms correct functioning as a straight-through cable.	1
	Student removes RJ45 and cuts cable short of where the split along the cable is no longer on the cable.	1

Fault	Steps taken by student	Marks
Cable 3: cable has been crimped but cables are short of the connectors at the end of the RJ45	Student correctly configures wires for straight-through cable.	1
	Student correctly crimps RJ45 with outer covering gripped by crimp.	1
	Student tests cable and confirms correct functioning as a straight-through cable.	1
	Student removes RJ45 to remove cracked connector and cuts wires to the correct length to ensure a correct fit.	1
Cable 4: the blue wire inside the twisted pair cable was accidently cut off when it was first terminated	Student correctly configures wires for straight-through cable.	1
	Student correctly crimps RJ45 with outer covering gripped by crimp.	1
	Student tests cable and confirms correct functioning as a straight-through cable.	1
	Student removes the T-568A end.	1
Cable 5: cable was terminated incorrectly, which allows the twisted pair cable to be removed from the RJ45 connector	Student correctly configures wires for straight-through cable.	1
	Student correctly crimps RJ45 with outer covering gripped by crimp.	1
	Student tests cable and confirms correct functioning as a straight-through cable.	1

Fault	Steps taken by student	Marks
	Completion of test plan:	
	Test plan is completed consistently, accurately and with relevant and logical remarks.	5–6
	Test plan is completed, although there may be some less important issues missed. Remarks are mixed, with some relevant but not all.	3–4
	There is limited information in the test plan. It may not be accurate and it may miss important elements.	1–2
	No creditworthy material.	0

Task 2: troubleshooting the proposed cabling installation

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

Band	Mark	Descriptor
4	13–16	Comprehensive testing of the Cisco Packet Tracer network and exceptional ability to troubleshoot and fix any issues encountered. All issues have been identified and resolved.
3	9–12	Proficient testing of the Cisco Packet Tracer network and effective ability to troubleshoot and fix any issues encountered. All issues have been identified and the majority of these have been resolved.
2	5–8	Some testing of the Cisco Packet Tracer network, which may be seen as sufficient at the top of the band but may not be adequate at the bottom of the band. Some ability to troubleshoot and fix any issues encountered but may have only resolved some issues.
1	1–4	Limited testing of the Cisco Packet Tracer network. Limited ability to troubleshoot and fix any issues encountered.
0	0	No creditworthy material.

Indicative content

The student has carried out cable testing, applying appropriate testing tools, in accordance with the manufacturer's equipment procedures and in compliance with TIA/EIA standards.

Cisco Packet Tracer testing tools are used to carry out or address, for example:

- add simple PDU
- add complex PDU
- device properties
- CLI (for example, ICMP or traceroute)

Cisco Packet Tracer troubleshooting covers, for example:

- correct IP addressing

- correct subnet masks
- correct cable connection types
- port status turned on for:
  - network cards in PC
  - routers
  - switches
  - servers

Known faults on the system include:

- server connected via WiFi rather than Ethernet
- laptop not connected to wireless
- main office printer set to DHCP
- PC1 in main office set to static IP with no detail filled in
- wireless tablet not connected to network
- 'work' network has no security

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

PO3: Discover, evaluate and apply reliable sources of knowledge

Band	Mark	Descriptor
4	4	The test plan and written description of analysis show exceptional and, at the top of the band, very comprehensive critical thinking regarding the choices and decisions during the testing process.
3	3	The test plan and written description of analysis show a good amount of effective critical thinking regarding the choices and decisions during the testing process, covering most of the key elements.
2	2	The test plan and written description of analysis show some critical thinking regarding the choices and decisions during the testing process but may miss some key elements.
1	1	The test plan and written description of analysis show limited or very limited critical thinking regarding the choices and decisions during the testing process.
0	0	No creditworthy material.

Indicative content

Critical thinking can be demonstrated through the test plan and written description of analysis, which would consider the process of critical thinking and the application of evaluation techniques and tools.

The quality of the student's test plan will be in line with their ability to identify faults in this task.

The quality of the student's written description of analysis will be in line with their ability to resolve faults in this task.

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

Task 3: carry out a risk assessment of the client's network

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

Band	Mark	Descriptor
4	10–12	The student identifies a comprehensive range of risks related to the scenario, which must include examples of physical, technical and administrative risks. The student makes excellent recommendations for security controls and comprehensively identifies the physical, technical and administrative controls as part of their risk assessment.
3	7–9	The student identifies a good range of risks but may not include all and may miss some less important risks. The student makes good recommendations for security controls and identifies a wide range of physical, technical and administrative controls as part of their risk assessment.
2	4–6	The student identifies some risks, which include some key ones, but may also miss some key risks. The student makes sound recommendations for security controls and identifies some physical, technical and administrative controls as part of their risk assessment.
1	1–3	The student identifies a limited number of risks and has missed most of the key risks. The student makes a few basic recommendations for security controls and identifies a limited number of physical, technical and administrative controls as part of their risk assessment.
0	0	No creditworthy material.

Indicative content

- risk assessment template has been completed, including physical, technical and administrative risks
- all columns contain appropriate explanations. Impact and likelihood contain low/medium/high/critical qualitative rating
- actions are identified with detailed explanations of how the actions taken will mitigate risks
- controls should be identified as technical, physical or administrative

- actions should be detailed as preventative, detective, corrective, deterrent, directive, compensating or acceptance

The student should identify a range of risks to the network based on the scenario. These may include:

- GDPR could be breached, as clients when waiting are able to hear sales staff have conversations with other clients
- there is only one door into the building, and this is not ideal in the event of a natural disaster
- no appearance of security to stop people wandering into the office via the front door
- there is a single point of failure with only having a single router
- the router is responsible for multiple roles (DHCP server and firewall)
- the wireless network is detectable by a wireless analyser 15m outside the office, which may lead to potentially malicious access
- 2-factor authentication (2FA) is needed on staff accounts to provide more security
- the building is in an area with lots of footfall and crime is on the rise due to living costs
- no backup internet connection
- no fire protection for the server
- sprinkler system could flood the building, especially given that there is a false floor
- the scenario implies that there is no managed access to the server room and no real building control for closing the building; this could result in accidentally leaving the building open – loss of keys is a significant risk
- single point of failure to the server due to only one implemented network card

Mitigations should be valid and should not be out of the realms of practicality/reasonable expense.

Physical controls could be implemented in appropriate areas based on the scenario given. Examples could include:

- poor access control, such as key fobs
- Kensington locks
- security alarms
- security guards on site
- secure server room
- CCTV
- external fence or gate
- ID cards

Technical controls could include:

- installation of antivirus or malware software
- WiFi encryption
- patch management
- additional unused network cards could provide redundancy

- 2FA

Administrative controls could include:

- sign in/sign out procedures
- acceptable use policy
- password policy

Accept any other suitable responses.

In this scenario, the student could also consider other physical controls such as:

- cables in the office – where are the cables located? Are they in protective trunking or visible?
- what are the risks of having no physical security measures in place?
- what are the risks of being located in the middle of a city centre?

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

Example risk assessment with some entries completed:

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
Rodents and wildlife damaging cables	Unprotected and exposed external cabling.	Physical cables and data being transmitted.	Medium Loss of service to customer. Potential reputational damage for organisation. Additional cost for replacement of cables.	Medium Although the majority of cable is protected, some sections are exposed.	Cables are damaged by wildlife, leading to loss of service for client and damage to reputation for providing organisation.	Ensure physical trunking protects cables in their entirety. Implement methods to deter wildlife where needed.	Physical Preventative
Flooding	Ground floor equipment.	Physical assets with potential impact on digital assets.	High Damage to physical assets resulting in loss of digital data. This may result in downtime and have a financial impact.	Low The area is noted to not have any flooding and no mention of water mains within the building being near important areas.	Equipment being water damaged leading to loss of service.	As there is almost no risk, there are no applicable actions.	Acceptance

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
Loss of service – active directory	Server/service.	Digital services.	Medium Logging into devices will be impacted where not using cached accounts.	Medium As only one server offers this service for both networks, this is a single point of failure.	Loss of business-critical service resulting in a loss of productivity and potential financial impact.	Configure the alternative server to also act as a domain controller so as to avoid a single point of failure.	Preventative
Security breach between sites	The site-to-site connection.	Data communication between sites.	High Confidential data loss potentially resulting in GDPR issues.	Low Due to the site-to-site connection utilising a VPN connection to secure traffic between the 2 sites.	The site-to-site link is breached by a third party without authorisation.	To ensure the connection is not breached, regular monitoring of logs and scheduled changes to the pre-shared key used to secure the VPN.	Preventative Detective

PO3: Discover, evaluate and apply reliable sources of knowledge

Band	Mark	Descriptor
4	4	The recommendations provided demonstrate an excellent level of critical thinking in the generation of the security risk assessment and highly effective understanding of why the risk level is justified, with excellent explanation as to how the controls reduce the risk.
3	3	The recommendations provided demonstrate a good level of critical thinking in the generation of the security risk assessment and mostly effective understanding of why the risk level is justified, with good explanation as to how the controls reduce the risk.
2	2	The recommendations provided demonstrate a reasonable level of critical thinking in the generation of the security risk assessment and some understanding of why the risk level is justified, with reasonable explanation as to how the controls reduce the risk.
1	1	Any recommendations provided demonstrate a minimal level of critical thinking in the generation of the security risk assessment and basic understanding of why the risk level is justified, with limited explanation as to how the controls reduce the risk.
	0	No creditworthy material.

Indicative content

For each risk the student identifies, they should be fully completing the risk assessment template provided.

For example, the student could identify the following in relation to the risk of no managed access to the server room and no real building control for closing the building:

- identification of threat:
  - careless employees
- vulnerability related to threat:
  - loss of keys
- asset at risk:
  - services provided by the router – all assets, all infrastructure assets
- impact if threat is exploited:
  - GDPR breach depending on data lost
  - downtime – possible breach of service level agreement (SLA)
  - financial loss from theft and replacement of locks and keys
- likelihood that threat is exploited:
  - medium

- overall risk to business:
  - high
- recommended action:
  - implement key management (separate keys for separate locks)
- type of control:
  - physical

For other identified risks, a similar level of critical thinking should be applied to give a similar level of detail.

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	4	21		25
2		16	4	20
3	12		4	16
Total marks	16	37	8	61
% weighting	26%	61%	13%	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 watermark	November 2023	16 November 2023