T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 3

Mark scheme

Paper number: P001655
V1.0: Prestandardisation
Summer 2023
603/6901/2

NCFE

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

Digital Infrastructure

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 levels, 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 a relevant standardisation event 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

This assessment requires students to:

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

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure

PO3: Discover, evaluate and apply reliable sources of knowledge

Task 1

(20 marks)

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

Band	Mark	Descriptor
4	13–16	The student identifies a comprehensive range of vulnerabilities related to the scenario, which must include examples of physical, technical and administrative vulnerabilities/risks. The student makes sophisticated recommendations for security controls and comprehensively identifies the physical, technical and administrative controls as part of their risk assessment.
3	9–12	The student identifies a good range of vulnerabilities, but may not include all, and may miss some less important vulnerabilities. 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	5–8	The student identifies some vulnerabilities, which includes some key ones, but may also miss some key vulnerabilities. The student makes sound recommendations for security controls and identifies some physical, technical and administrative controls as part of their risk assessment.
1	1–4	The student identifies a limited number of vulnerabilities and has missed most of the key vulnerabilities. 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	No creditworthy material.

Indicative content

Risk assessment template has been completed including physical, technical and administrative risks.

Assets, impacts and likelihood contain appropriate explanations, as well as a low/medium/high/critical qualitative rating.

Actions are identified with detailed explanations of the actions taken. Risk reductions should be specified.

Controls should be identified as technical, physical or administrative.

Actions should be detailed as preventative, detective, corrective, deterrent, directive, compensating or acceptance.

Physical controls should be documented on the floor plan document. Examples could include:

- server room created
    - locked door system – keypad or swipe card
    - air conditioned
- access to public areas is monitored
- security guard
- mantrap
- door access control, such as key fobs
- Kensington desk locks in hot desk areas
- security alarm on fire door

Technical controls could include:

- improved account management
- audit of devices on network
- security policy updated on Group Policy Management
- installation of antivirus or malware software
- encryption
- EFS for individual files
- BitLocker or other disk encryption for laptops
- BitLocker To Go or removable drive encryption for removable media
- patch management
- configuring file and folder permissions

Administrative controls could include:

- sign in/sign out procedures
- no tailgating policy
- acceptable use policy
- password policy
- phishing/security training

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 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 form.

For example, if the identified risk is that the server is in a publicly accessible area, the student could identify the following:

- identification of threat
  - server is in a publicly accessible area
- vulnerability related to threat
  - an attacker could easily gain access to the physical server and access data on it, for example, by booting from a USB device with Kali Linux installed on it
- asset at risk
  - physical server, customer data, confidential business critical data
  - cloud security
- impact if threat is exploited
  - data leaked to competitors or to malicious actors
  - GDPR breach and consequent fines
  - critical data deleted from the server
- likelihood that threat is exploited
  - medium
- overall risk to business
  - high

- recommended action
    - relocation of server to a locked room with controlled access
    - disable USB ports on the server
- 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.

Task 2

(8 marks)

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

PO3: Discover, evaluate and apply reliable sources of knowledge

Band	Mark	Descriptor
4	7–8	The student has written an excellent administrative security recommendations report that comprehensively meets the scenario. The report includes: • a comprehensive list of security controls that are highly focused on the scenario and demonstrate highly effective evaluation skills • detailed descriptions of how the security controls will be enforced • relevant legislation, regulations or standards related to all controls, where appropriate
3	5–6	The student has written a good administrative security recommendations report that closely meets the scenario. The report includes: • a good range of security controls that are focused on the scenario, but may be missing some controls and demonstrate mostly effective evaluation skills • good descriptions of how the security controls will be enforced • relevant legislation, regulations or standards related to most controls, where appropriate
2	3–4	The student has written a satisfactory administrative security recommendations report that somewhat meets the scenario. The report includes: • a list of security controls that are sometimes focused on the scenario, but miss the important controls and demonstrate partially effective evaluation skills • reasonable descriptions of how the security controls will be enforced • relevant legislation, regulations or standards related to some controls, where appropriate

Band	Mark	Descriptor
1	1–2	The student has written a basic administrative security recommendations report that has limited relevance to the scenario. The report includes: • a limited or minimal list of security controls that have limited focus on the scenario and demonstrate only limited evidence of evaluation • brief descriptions of how the security controls will be enforced • relevant legislation, regulations or standards related to few controls, where appropriate
	0	No creditworthy material.

Indicative content

The student provides explanations of potential security controls that could be implemented and their reasons for choosing those controls.

This could include:

- password policy
  - ensuring passwords are hard to compromise and staff understand how best to keep passwords secure
- tailgating
  - preventing an intruder gaining unauthorised access to the site
- locking screens
  - preventing unauthorised access of a staff member's account while away from the computer
- encryption of mobile data
  - ensuring confidential data cannot be accessed in the event of theft or other loss
- mandatory training for staff
  - reduces user error or social engineering style attacks from giving access to company systems
- installation of firewall, antivirus or other antimalware software
  - reduces risk of malicious malware or viruses accidentally being installed on company computers

Controls should be accompanied by an explanation of their benefit to the business and how they can be used. Where appropriate students may reference legislation such as:

- Data Protection Act (2018)/GDPR
- Computer Misuse Act

Where appropriate, students may reference frameworks, standards or regulatory bodies such as:

- NCSC
- NIST
- OWASP
- ISO 27001

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

(8 marks)

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

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure

Band	Mark	Descriptor
4	7–8	The student has written an excellent and comprehensive disaster recovery recommendations document and uses appropriate examples extensively throughout to shape the document. The disaster recovery recommendations document is highly relevant to the scenario. The student has written an excellent and comprehensive business continuity recommendations document and uses appropriate examples extensively throughout to shape the document. The business continuity recommendations document is highly relevant to the scenario.
3	5–6	The student has written a clear disaster recovery recommendations document that may miss some less important elements and uses appropriate examples most of the time to shape the document. The disaster recovery recommendations document is relevant to the scenario. The student has written a clear business continuity recommendations document that may miss some less important elements and uses appropriate examples most of the time to shape the document. The business continuity recommendations document is relevant to the scenario.
2	3–4	The student has written a disaster recovery recommendations document that covers some of the key elements but not all and at the lower end of the band may not be effective. The student occasionally uses appropriate examples to shape the document. The disaster recovery recommendations document has some relevance to the scenario. The student has written a business continuity recommendations document that covers some of the key elements but not all and at the lower end of the band may not be effective. The student occasionally uses appropriate examples to shape the document. The business continuity recommendations document has some relevance to the scenario.
1	1–2	The student has written a basic or limited disaster recovery recommendations document and rarely uses appropriate examples to shape the document. The disaster recovery recommendations document has little relevance to the scenario. The student has written a basic or limited business continuity recommendations document and rarely uses appropriate examples to shape the document. The business continuity recommendations document has little relevance to the scenario.

Band	Mark	Descriptor
	0	No creditworthy material.

Indicative content

Disaster recovery - focuses on recommendations for what needs to happen to recover the IT infrastructure in case of a fire.

Suitable examples could include:

- monitoring systems and alarms
- restoration of back-up
- asset inventory/loss identification
- communication plan
- roles of staff in recovering site
- hot, warm or cold sites
- sequence of tasks to prioritise critical information
- recommissioning of site

Accept any other suitable responses.

Business continuity - focuses on recommendations for resuming/maintaining the IT infrastructure after a fire.

Suitable examples could include:

- failover to a remote site
- restoring back-ups
- patching software
- SLA call to repair equipment
- temporary premises
- temporary infrastructure brought on site
- cloud services to provide redundancy and continuity of teaching online

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

Task 4

(20 marks)

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

Band	Mark	Descriptor
4	13–16	The student takes steps to mitigate all the actions given in the assignment efficiently. They differentiate effectively between different types of hardware (desktop/server) and tailor their actions effectively to each setting. The security controls implemented will protect the system and are fully relevant to the scenario.
3	9–12	The student takes steps to mitigate most of the actions given in the assignment. They show good differentiation between different types of hardware (desktop/server) and tailor some of their actions to each setting. The security controls implemented will protect the system and are mostly relevant to the scenario but may miss some less important elements.
2	5–8	The student takes steps to mitigate some of the actions given in the assignment (including antivirus software). They show little differentiation between different types of hardware (desktop/server) and show little tailoring of their actions to each setting. The security controls implemented will protect the system but may not always be relevant to the scenario and may miss key elements.
1	1–4	The student takes steps to mitigate a limited number of the actions given in the assignment (including antivirus software). They show no differentiation between different types of hardware (desktop/server) and show little to no tailoring of their actions to each setting. The student provides basic or limited security controls to protect the system, which may not be relevant to the scenario and may miss many key elements.
	0	No creditworthy material.

Indicative content

The student produces evidence that demonstrates mitigation of each action in the assignment brief. Examples of appropriate mitigations could include:

- (action 1) appropriate encryption is implemented to protect data that may be removed from site
    - appropriate use of drive encryption, such as BitLocker
    - removable drives configured with encryption, such as BitLocker To Go
- (action 2) finance files should be encrypted at all times
    - EFS used for encrypting finance documents
    - devices configured with encryption, such as BitLocker To Go
- (action 3) appropriate antivirus and malware protection are implemented correctly
    - student sources and installs appropriate antivirus software such as Avast/Avira/AVG/Windows Defender
    - student sources and installs appropriate antimalware software such as Malwarebytes
    - virus scan runs and Eicar is removed
- (action 4) operating system vulnerabilities are mitigated against
    - Windows updates are configured/other patch management
- (action 5) user accounts are only able to access appropriate files and folders
    - user accounts are added to groups and permissions to resources are configured appropriately
    - student could provide 2 print screens showing an authorised account accessing a resource **and** an unauthorised account being prevented from accessing the same resource
- (action 6) an appropriate password policy is in place
    - complex passwords are enforced through GPO or similar

The student also provides an explanation of why they have carried out each of these tasks and the benefits they expect to gain from the actions taken.

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 explanations provided demonstrate an excellent level of critical thinking regarding the implementation of the security controls, with highly effective evaluation.
3	3	The explanations provided demonstrate a good level of critical thinking regarding the implementation of the security controls, with mostly effective evaluation.
2	2	The explanations provided demonstrate a reasonable level of critical thinking regarding the implementation of the security controls, with some evidence of evaluation that is partially effective.
1	1	Any explanations provided demonstrate a minimal level of critical thinking regarding the implementation of the security controls, with only limited evidence of evaluation.
	0	No creditworthy material.

Indicative content

Examples of explanations demonstrating critical thinking for each action could include:

- (action 1) appropriate encryption is implemented to protect data that may be removed from site
  - BitLocker drive encryption will prevent access to any data on the drive if it is physically removed from the computer
- (action 2) finance files should be encrypted at all times
  - EFS encryption ties the document to the owner's digital certificate, preventing any other user from accessing the file or folder
- (action 3) appropriate antivirus and malware protection are implemented correctly
  - antivirus software will identify any virus that is copied or downloaded onto the computer or is resident on any removable media attached
  - heuristic software will adapt and identify common virus patterns to reduce risk of an unknown virus compromising the computer
  - antimalware software is similar but protects against a wider range of malware threats including spyware and ransomware
- (action 4) operating system vulnerabilities are mitigated against
  - Windows updates download the latest patches for the operating system, including patches for recently identified vulnerabilities that could compromise the computer in some way
- (action 5) user accounts are only able to access appropriate files and folders
  - it is important that individual users can only access data that they are authorised to see; for instance, it would be inappropriate for users to see each other's payroll or HR files
- (action 6) an appropriate password policy is in place
  - a good password policy will specify that complex passwords are in use to reduce the risk of a password being cracked or brute forced

- it will also give guidance to users on how to create an appropriate password, how often passwords should be changed and whether passwords can be reused
- it will also give guidance to protect from passwords being leaked through them being written down or shared
- it will minimise the risk of passwords being lost or compromised as a result

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	16		4	20
2	6		2	8
3	4	4		8
4	16		4	20
Total marks	42	4	10	56
% Weighting	75%	7%	18%	100%

Document information

Owner: Head of Assessment Design.