

# T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

## Digital Support

Assignment 3

Mark scheme

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

# Digital Support

### Mark scheme

Assignment 3

## Contents

|  |           |
|--|-----------|
| <b>Marking guidelines</b> .....            | <b>3</b>  |
| <b>Task 1</b> .....                        | <b>5</b>  |
| <b>Task 2</b> .....                        | <b>8</b>  |
| <b>Performance outcome (PO) grid</b> ..... | <b>10</b> |
| <b>Document information</b> .....          | <b>11</b> |
| Change History Record .....                | 11        |

# 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 determine 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

SAMPLE

# Task 1

(12 marks)

| Band | Mark  | Descriptor   |
|------|-------|--|
| 4    | 10–12 | <p>Excellent annotated screenshots/photographs and maintenance notes that cover all installations and have a high level of detail.</p> <p>The infrastructure log is detailed, and testing is comprehensive.</p> <p>Accurately completed penetration test remediation log demonstrating in-depth analysis of penetration test report.</p> <p>All 21 vulnerabilities transferred along with proposed, well-reasoned mitigation.</p> <p>Future planning is exceptional and fully considers the penetration test report.</p> |
| 3    | 7–9   | <p>Good annotated screenshots/photographs and maintenance notes that cover all installations in good detail.</p> <p>Infrastructure log is sufficient, and testing is detailed.</p> <p>Completed penetration test remediation log with minor omission/errors demonstrating good analysis of penetration test report.</p> <p>All 21 vulnerabilities transferred but some proposed mitigation either missing or vague.</p> <p>Future planning is in-depth and considers the penetration test.</p>                           |
| 2    | 4–6   | <p>Reasonable screenshots/photographs and maintenance notes that cover most installations in some detail.</p> <p>Infrastructure log is basic, and testing is sound.</p> <p>Completed penetration test remediation log with some omissions/errors demonstrating reasonable analysis of penetration test report.</p> <p>All critical and high vulnerabilities transferred but some medium missed.</p> <p>Future plan provided with some consideration for the penetration test.</p>  |
| 1    | 1–3   | <p>Poor maintenance notes that are lacking in detail.</p> <p>Infrastructure status log is insufficient.</p> <p>Poorly completed penetration test remediation log demonstrating limited analysis of penetration test report.</p> <p>Missing some critical or high vulnerabilities.</p> <p>No consideration of the penetration test.</p>   |
|      | 0     | No creditworthy material.  |

## Indicative content




Student's evidence may include:



- purpose and approach of testing
- industry standard and regulatory compliance
- techniques applied to security for internet connected devices, systems and networks
- interpreting results of penetration testing
- status reporting and updating
- security methods
- infrastructure status log
- test and execution
- types of impacts as a result of vulnerabilities
- identifying potential threats and vulnerabilities in critical systems
- measures and procedures to mitigate threats and vulnerabilities
- future planning

The following section is presented as marking scheme guidance when marking the penetration test report. It is provided to remove the need for a marker to have detailed knowledge of penetration testing.

Students should analyse the contents of the report paying special attention to the severity of a vulnerability.

The table below shows the CVSS rating for the vulnerabilities found, it should be noted that critical and high vulnerabilities pose a serious security threat to any affected system. This is because they usually relate to known exploits where sample code and methods of leveraging the exploit are readily available.

| Symbol  | Risk rating | CVSSv2 score range | Explanation   |
|---|-------------|--------------------|---|
|  | CRITICAL    | 9.0 to 10.0        | A vulnerability has been discovered that is rated as CRITICAL. This could mean that the system may be exposed to a known exploit allowing catastrophic damage/data breach. Company A has advised that these issues need immediate resolution in < 3 days.   |
|  | HIGH        | 7.0 to 8.9         | A vulnerability has been discovered that is rated as HIGH. This could mean that the system has known vulnerabilities which could expose the associated system allowing unauthorised access. This requires a resolution in the short term and company A has agreed that these issues need to be resolved in < 25 days.             |
|  | MEDIUM      | 4.0 to 6.9         | A vulnerability has been discovered that is rated as MEDIUM. This could mean that the system has known medium level vulnerabilities linked to maintenance such as missing security patches. Company A has advised that these issues should be addressed as part of the next maintenance cycle (for example system patch updates). |

| Symbol  | Risk rating | CVSSv2 score range | Explanation   |
|---|-------------|--------------------|---|
|  | LOW         | 1.0 to 3.9         | A vulnerability has been discovered that is rated as LOW. This could mean that the system has known low level vulnerabilities linked to maintenance such as missing security patches. Company A has advised that these issues should be addressed as part of the next maintenance cycle (for example system patch updates). |
|  | INFO        | 0 to 0.99          | A vulnerability has been discovered that is rated as INFORMATIONAL. This could mean that the system is not following best practice and should be reviewed for appropriate action.   |

## Number of vulnerabilities

When analysing a penetration test report, it is essential that all relevant vulnerabilities are transferred to the pen test remediation log regardless of severity (although actions to mitigate the more severe issues should be carried out immediately).

The table below shows the number and severity of the vulnerabilities, discovered, marks should be awarded as follows:

- band 4 - all 21 vulnerabilities transferred along with proposed, well-reasoned mitigation
- band 3 - all 21 vulnerabilities transferred but some proposed mitigation either missing or vague
- band 2 - all critical and high vulnerabilities transferred but some medium missed
- band 1 - missing some critical or high vulnerabilities

| Area           | Critical | High | Medium | Low | Total |
|----------------|----------|------|--------|-----|-------|
| Workstations   | 0        | 4    | 1      | 0   | 5     |
| Servers        | 1        | 10   | 0      | 0   | 11    |
| HP Printers    | 0        | 0    | 5      | 0   | 5     |
| <b>Totals:</b> | 1        | 14   | 6      | 0   | 21    |

## Task 2

(15 marks)

| <b>Demonstrate deployment of software applications and operating systems remotely:</b>  |           |  |
|---|-----------|--|
| Create an image: <ul style="list-style-type: none"> <li>install and configure operating system</li> <li>application installation</li> <li>active directory</li> <li>deployment task sequence</li> </ul>   | 4         | Award 1 mark for each set of screenshots/evidence  |
| Upload image to distribution system   | 2         | Award 1 mark for image being available<br>Award 2 marks for image being available and ready for deployment   |
| Deploy and test image: <ul style="list-style-type: none"> <li>deploy image from distribution system</li> <li>log into client and test network connectivity</li> <li>check image quality and all applications are functioning as expected</li> </ul> | 3         | Award 1 mark for each set of screenshots/evidence  |
| <b>Test plan and test log:</b>  |           |  |
| Testing   | 3         | Award marks for the following descriptors:<br>1 - basic windows functionality testing<br>2 - good windows functionality testing and application testing<br>3 - extensive windows functionality testing, application testing and evidence that the windows event log has been accessed and any issues noted |
| Correct use of terminology used throughout  | 3         | Award marks as per following descriptors:<br>1 - some use<br>2 - good use<br>3 - excellent use   |
| <b>Total marks</b>  | <b>15</b> |  |



## Indicative content

Student's evidence should include:

- steps in creating image
- system requirements
- hardware configuration
- methods of installation and deployment
- boot methods
- partitioning
- file system types
- file system formatting
- installation and deployment of software
- applying updates
- testing deployment meets requirements

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

- system
- workstation
- image
- deployment
- active directory
- operating system
- application software
- hardware
- task sequence
- configuration
- back-up measures
- application types
- upgrades
- installation

## Performance outcome (PO) grid

| Task               | PO1 | PO2 | PO3 | Total |
|--------------------|-----|-----|-----|-------|
| 1                  | 3   | 7   | 2   | 12    |
| 2                  | 1   | 10  | 4   | 15    |
| <b>Total marks</b> | 4   | 17  | 6   | 27    |
| <b>% weighting</b> | 15% | 63% | 22% | 100%  |

SAMPLE

## Document information

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2020-2023.

'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    | Post approval, updated for publication.              |               | December 2020    |
| v1.1    | Branding and formatting final updates. NCFE rebrand. |               | September 2021   |
| v1.2    | Sample added as a watermark.                         | November 2023 | 20 November 2023 |