T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 3

Mark scheme

Paper number: P001662
Summer 2023
603/6901/2

T Level Technical Qualification in Digital Support Services Occupational specialism assessment (OSA) (603/6901/2)

Digital Support

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 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 bands, 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

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

(12 marks)

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

Task 2

(15 marks)

Demonstrate deployment of software applications and operating systems remotely:		
Create an image: • install and configure operating system • application installation • active directory • deployment task sequence	4	Award 1 mark for each set of screenshots/evidence
Upload image to distribution system	2	Award 1 mark for image being available Award 2 marks for image being available and ready for deployment
Deploy and test image: • deploy image from distribution system • log into client and test network connectivity • check image quality and all applications are functioning as expected	3	Award 1 mark for each set of screenshots/evidence
Test plan and test log:		
Testing	3	Award marks for the following descriptors: 1 - basic windows functionality testing 2 - good windows functionality testing and application testing 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: 1 - some use 2 - good use 3 - excellent use
Total marks	15	

Indicative content

Student's evidence should include, but is not limited to:

- steps in creating image

- system requirements
- hardware configuration
- methods of installation and deployment
    - office application – such as MS Office, Libre Office, Open Office
    - PDF reader – such as Adobe Acrobat Reader
    - anti-virus software – such as AVG Free
    - software development suite – such as Notepad++ or MS Visual Studio
- 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 and may include, but is not limited to:

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

Performance outcome grid

Task	PO1	PO2	PO3	Total
1	3	7	2	12
2	1	10	4	15
Total marks	4	17	6	27
% Weighting	15%	63%	22%	100%

Document information

Owner: Head of Assessment Design