T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 3

Project brief

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

Digital Support

Assignment brief

Assignment 3

Contents

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider during a set 2 week window.

The assignment will be completed under supervised conditions.

You must complete all tasks in this assignment independently. You are required to sign a declaration of authenticity to confirm that the work is your own. This is to ensure authenticity and to prevent potential malpractice and maladministration. If any evidence was found not to be your own work, it could impact your overall grade.

Internet access is available to allow you to access developer notes and help pages and to install, configure and update operating system, drivers and software applications and deploy them remotely. You are **not** permitted to use the internet for any other purpose, such as research. A copy of your browsing history must be submitted as part of your evidence for this assignment.

You have 10 hours to complete all tasks within this assignment. Each task has the following number of hours:

Task 1 = 6 hours (this task will be spread over 2 days).

Task 2 = 4 hours (this will be provided after completion of task 1 and be completed in one day).

Individual tasks must be completed within the timescales stated within each task, but it is up to you how long you spend on each part of the task, therefore be careful to manage your time appropriately.

Total marks available across all assignment 3 tasks = 27.

Details on the marks available are provided in each task.

You should attempt to complete all of the tasks.

Read the instructions provided carefully.

Take all photographs using the digital camera supplied by your provider. Use of mobile phones is **not** permitted.

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

Scenario

An efficient and functional system depends on monitoring and maintaining all infrastructure. At the same time, it is important to document the process. During this process you will analyse a recent penetration test report that has been produced about a network. This will lead you to identify vulnerabilities, provide solutions and identify trends and underlying problems. All of these will be documented in a continuous improvement plan.

To save time and improve efficiency, you must also create and deploy an image remotely. This will consist of an operating system and software applications.

Task 1: network analysis

Time limit

6 hours

You can use this time how you want.

(12 marks)

Student instructions

In this assignment you need to monitor, maintain, and demonstrate continuous improvement of a network. For this, you will need to complete an infrastructure status log. You have been provided with a list of equipment and a network overview diagram to help you complete your log.

You should complete all fields on the infrastructure status log including maintenance notes for the equipment. All of the information you need for this is included in appendix 3:

- worksheet 1 - infrastructure status log
- worksheet 2 - equipment list.

You must also analyse the penetration test report (appendix 5). You should record your findings and solutions in the penetration test remediation log (worksheet 3 in appendix 3). You need to include how current and future vulnerabilities will be mitigated. You also need to identify trends and identify underlying problems so that solutions are produced faster.

You need to provide evidence, where applicable, to justify your work and any future planning, this could be details from the penetration test report, your infrastructure status log, or the network overview diagram.

1) The evidence you should produce is:

- completed infrastructure status log
    - using the equipment list provided
    - showing maintenance notes for the installations
- analysis of penetration testing report
    - penetration test remediation log
    - mitigation of vulnerabilities
    - future planning, identifying trends and documenting underlying problems

You will have access to the following equipment:

- 1 x workstation set-up with office software installed
- internet access for developer notes and help pages

Evidence required for submission to NCFE

The following evidence should be submitted:

- infrastructure status log (worksheet 1 in appendix 3)
- penetration test remediation log (worksheet 3 in appendix 3)

- mitigation of vulnerabilities/planned improvements (word processed document)

- internet browsing history

Task 2: deploy image remotely

Time limit

4 hours

You can use this time how you want.

(15 marks)

Instructions for students

New software applications are needed for computers in an office. To save time and increase efficiency, these will be deployed remotely.

For this task, you need to complete a test plan and test log (worksheets 4 & 5 in appendix 3). This is needed because the image may need to be used on different hardware platforms (for example, graphic cards). This is necessary to make sure the deployed image is acting as expected.

You must create an image for machines for a group of software developers. They will need a productivity suite and appropriate software to be installed which includes an operating system, office software applications, drivers, rules, active directory permissions and a deployment task sequence. You will deploy this remotely.

You need to show that you have created and used an image remotely for **one** virtual or physical machine. The requirements include:

- create an image
- operating system:
  - all latest updates
- software applications:
  - office application
  - PDF reader
  - anti-virus software
  - software development suite
- active directory joined
- deployment task sequence
- upload image to image distribution system and make it available (for example, windows deployment service (WDS)
- deploy image
- create a test plan and complete log

You need to take screenshots and notes throughout the creation, deployment and testing of the image.

You can do this either virtually or physically.

You will have access to the following equipment:

- machine running WDS or similar

- internet access for developer notes and help pages

- one end-user device or virtual machine

- access to servers, network devices, network-based services

- an operating system and office applications for basic image deployment

- software development suite/software

- a digital camera

Evidence required for submission to NCFE

The following evidence should be submitted:

- annotated screenshots or photographs and documented notes showing creation and deployment of image

- test plan (worksheet 4 in appendix 3)

- test log (worksheet 5 in appendix 3)

- internet browsing history

Document information

Owner: Head of Assessment Design