T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 3

Assignment brief

v1.2: Specimen assessment materials
17 November 2023
603/6901/2

Internal reference: DSS-0006-01

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

Digital Infrastructure

Assignment brief

Assignment 3

Contents

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider over 2 days. The times and dates will be specified by NCFE.

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 only allowed for task 4.

Use the electronic workbook provided to record all your evidence against each task.

Annotations should be made digitally on the floor plan in the workbook.

Ensure all print screens have been labelled with a brief description of what is being shown.

Save your workbook regularly as you work through the assessment.

Submit the workbook as a single .pdf file at the end of the assessment.

Timing

You have 5 hours 30 minutes to complete all tasks within this assignment.

Task 1 = 2 hours (this will be completed in 1 session)

Task 2 = 45 minutes (this will be provided after completion of task 1 and is to be completed in 1 session)

Task 3 = 45 minutes (this will be provided after completion of task 2 and is to be completed in 1 session)

Task 4 = 2 hours (this will be provided after completion of task 3 and is to be completed in 1 session)

Individual tasks must be completed within the timescales stated for 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.

Marks available

Across all assignment 3 tasks: 56 marks.

Details on the marks available are provided in each task.

You should attempt to complete all of the tasks.

Read the instructions provided carefully.

Performance outcomes

Marks will be awarded against the skills and knowledge performance outcomes (POs) as follows:

Task 1

(20 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (16 marks)

PO3: Discover, evaluate and apply reliable sources of knowledge (4 marks)

Task 2

(8 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (6 marks)

PO3: Discover, evaluate and apply reliable sources of knowledge (2 marks)

Task 3

(8 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (4 marks)

PO2: Explain, install, configure, test and manage both physical and virtual infrastructure (4 marks)

Task 4

(20 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (16 marks)

PO3: Discover, evaluate and apply reliable sources of knowledge (4 marks)

Scenario

You are working as an infrastructure technician for Willow Technology and have been asked to evaluate the LAN being introduced to a new office located in York.

Willow Technology has a large number of staff that are remote workers. There is a small administrative team based in the York office along with an IT support team. Remote workers visit the site regularly to get access to the network and use the hot desks. Currently, the reception is open plan with a sign-in book on the desk and is only manned part time. With the large number of remote workers, different faces drop into site regularly. Only the site manager and IT teams have their own office.

The site has 3 entrances: a double-fronted reception, a staff entrance and a fire door at the rear of the building. None of these entrances are alarmed currently. The building is surrounded by a car parking area that currently has no restrictions to access in or out. Your manager is interested in the possibility of introducing surveillance on site.

Willow Technology will have 1 server located on site with the following roles:

- file server
- domain controller
- DHCP server
- DNS server
- print server

Location-based staff are issued with desktop PCs for their work, while remote staff are issued with company laptops.

Task 1

Time limit

2 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

(20 marks)

Currently the following user accounts have been configured on the network:

Server

Computer name: **Willow-DC01**

Local administrator: **Administrator/Pa$$w0rd**

Desktop PC

Computer name: **Willow-PC01**

Local administrator: **Willow-Admin/Pa$$w0rd**

Active Directory users

Louisa Warren (finance) **Louisa.Warren/Pa$$w0rd**

Bonnie Grace (HR manager) **Bonnie.Grace/Pa$$w0rd**

Jamal Turner (reception) **Jamal.Turner/Pa$$w0rd**

Dan Troke (sales director) **Dan.Troke/Pa$$w0rd**

Josh Smith (IT technician) **Josh.Smith/Pa$$w0rd**

Active Directory groups

Administrator – members Josh Smith and Dan Troke

Instructions for students

You have been provided with a copy of the floor plan for the York office and a security risk assessment template. Your manager has also provided you with the server and a client PC that will be used by staff on the network.

Your manager has asked you to evaluate the site and network with regards to cyber security to ensure that company resources and data are fully protected.

Perform a security risk assessment on the site and network recommending physical, administrative and technical controls. Explain why your recommendations will protect the network.

Your security risk assessment should include:

- identification of threat
- vulnerability related to threat
- asset at risk
- impact if threat is exploited

- likelihood that threat is exploited
- overall risk to business
- recommended action
- type of control

You should consider:

- the information provided in the scenario
- the York office floor plan
- the security on the server and client computer
- security risks that could occur because there is currently no documentation in place

Where appropriate you should annotate the floor plan to reflect any controls you have recommended as part of your risk assessment.

You will have access to the following equipment:

- word processing software
- virtual server and client PC

Evidence required for submission to NCFE:

- completed risk assessment document
- annotated floor plan

Task 2

Time limit

45 minutes

You can use the time how you want but all parts of the task must be completed within the time limit.

(8 marks)

Willow Technology currently has no documented security policies in place and your manager is concerned this represents a serious security risk. They have asked you to consider what administrative security policies are needed to best protect the company's customer data from being leaked, either accidentally or deliberately.

Instructions for students

To assist your manager in writing a security policy document, they have asked you to consider the kinds of controls that should be included in a security policy. You should submit a report that includes recommendations for controls that could be included in a security policy.

Your report should include:

- administrative controls to be implemented and your reasons for choosing these controls
- a description of how each control will be enforced within the business
- a note of any legislation, regulations or standards related to each control, where appropriate

You will have access to the following equipment:

- word processing software

Evidence required for submission to NCFE:

Report containing recommendations for the security policy.

Task 3

Time limit

45 minutes

You can use the time how you want but all parts of the task must be completed within the time limit.

(8 marks)

Recently there has been flooding near the site of the new office. Your manager is concerned that further flooding in the future could adversely affect the business. They are considering how well the business would cope if this were to happen. They are concerned the business has no policies or procedures in place to deal with this kind of emergency.

Instructions for students

Your manager has asked you to recommend a range of actions that could be taken to provide business continuity and support disaster recovery from a flood in a timely manner, whilst protecting systems and data. Your manager would like to have the business operational within 3 days of a major disaster. The business is willing to invest a substantial budget for this project. You should focus on recommendations that maintain business continuity and restoring operations ahead of financial concerns.

You need to write:

- a business continuity document with your recommendations in the case of flooding
- a disaster recovery document with your recommendations in the case of flooding

You will have access to the following equipment:

- word processing software

Evidence required for submission to NCFE:

- business continuity recommendations document
- disaster recovery recommendations document

Task 4

Time limit

2 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

(20 marks)

Instructions for students

Your manager has asked you to consider how the server and client PC can be hardened to better protect the company network and data, and to make these changes.

You need to ensure that the network is fit for purpose and that company resources are secure and protected at all times.

Actions taken should include:

- appropriate encryption to be implemented to protect data that may be removed from site
- finance files should be encrypted at all times
- appropriate antivirus and malware protection are implemented correctly
- operating system vulnerabilities are mitigated against
- user accounts are only able to access appropriate files and folders
- an appropriate password policy is in place

You should consider the following information: Current systems configuration

Server

Operating system:

- Windows Server 2016 Datacenter Edition (With GUI)

Server roles:

- DHCP
- DNS
- Active Directory domain controller
- file and print server

Firewall:

- Windows Firewall – no configuration beyond windows defaults have been applied

Antivirus:

- none

Installed software:

- no additional software has been installed

Desktop client PC

Operating system:

- Windows 10 Professional

Firewall:

- Windows Firewall – no configuration beyond windows defaults have been applied

Antivirus:

- Windows defender – disabled

Installed software:

- OpenOffice 4.1.7

Encryption:

- no encryption has been applied

Note: Internet access is available for this task to allow you to download any software that you consider necessary to secure or harden the server, according to the action list above. 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 task.

You will have access to the following equipment:

- word processing software
- virtual server and client PC

Evidence required for submission to NCFE

For each action you need to submit evidence of:

- the action you have chosen to implement
- screenshots of server and/or client before the configuration change, during the change and after the change (the reconfigured system)
- a note of any unexpected results found whilst hardening the system
- an explanation of how the action you have taken will better protect the system
- a copy of your browsing history showing the websites you have accessed

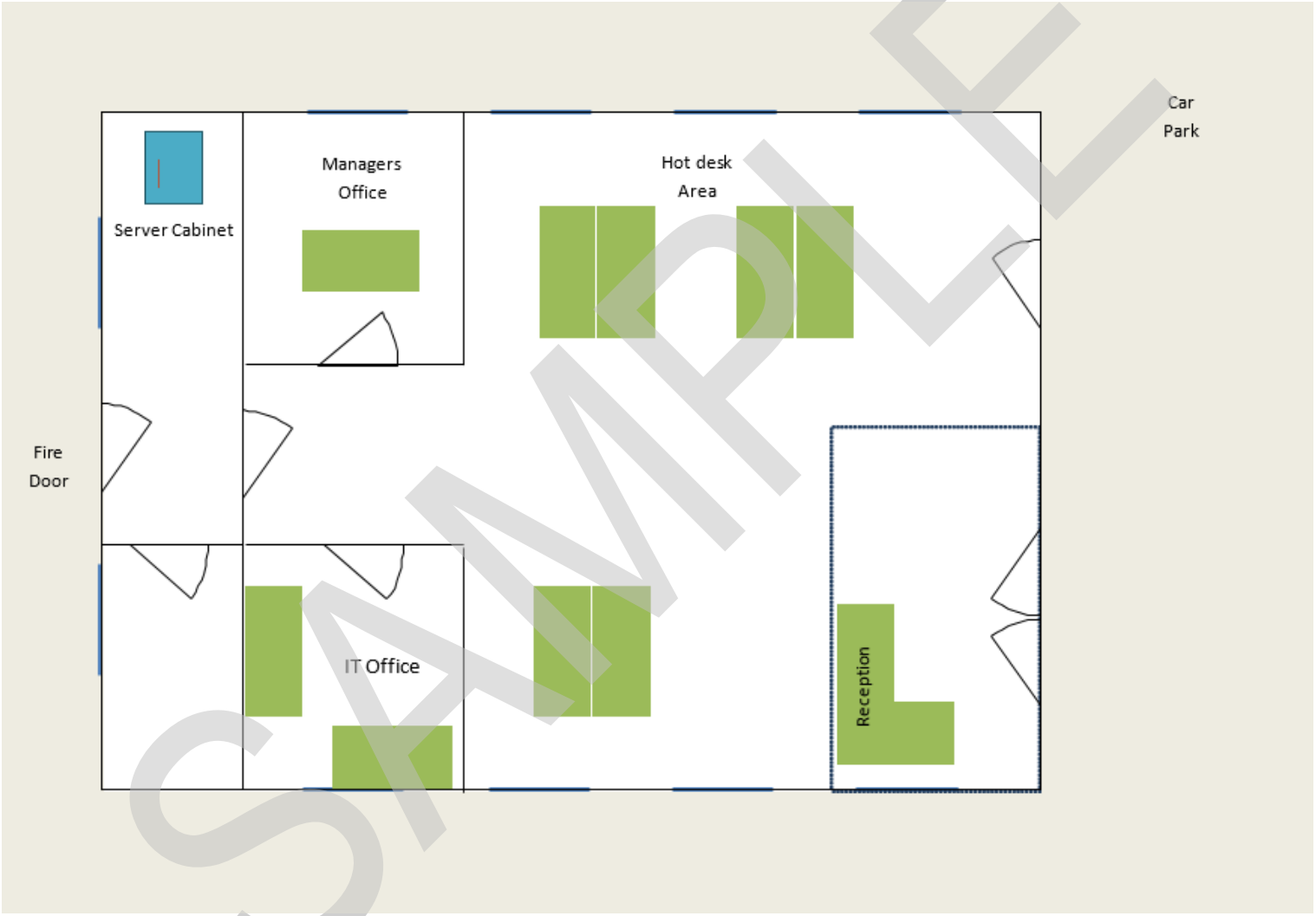
All print screens should be numbered and linked to the task as stated in electronic workbooks

Risk assessment template

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
Such as passwords cracked by attacker	Lack of password complexity policy	Files or data on file shares High	Critical data could be accessed by a malicious attacker and stolen Critical	Attackers would need access to the network or password hash to attempt this Medium	Data is exfiltrated from the company with potential to damage company reputation, breach of GDPR with financial implications and potential for customers becoming victims of identity theft High	Implement complex password policy in directory services	Technical/ preventative

Risk levels:	Business control types:	Mitigating control types:
low | medium | high | critical	physical | administrative | technical	preventative | detective | corrective | deterrent | directive | compensating | acceptance

York office floor plan



Document information

The T Level Technical Qualification is a qualification approved and managed by 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	17 November 2023