T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 3

Assignment brief

v1.1: Additional sample material
17 November 2023
603/6901/2

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. 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 4 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 (POs)

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

As a recently hired infrastructure technician for DoubleUp Bookkeeping, you have been asked to investigate the network infrastructure for the company.

DoubleUp Bookkeeping has completed the merger of 2 buildings. It now has 7 offices, a meeting room, a server room and a reception area. As a result of predicted growth, each office should be able to accommodate 2 accountants. The building is on a single floor with a public reception. Only the reception is open to the public; however, there are unsecured access doors that lead to the main office space. Specific accountancy staff need access to the 7 offices within the building 24 hours a day, 7 days a week. There is no current monitoring or access system in place. The normal working hours of the building are Monday to Friday, 09:00am to5:30pm. Currently, no doors apart from the doors at reception have any form of locks or access prevention.

The site has a main front entrance leading to the reception and multiple fire exits that are located around the building. At present, there are 5 security cameras to monitor the outside of the building. There is, however, no alarm system installed on site. The current network design and configuration documentation was created before the merger of the 2 buildings and is outdated. It has been noted that the junior members of the team are using the network connected devices to go onto social media platforms – this is to be restricted for all users. Due to the heat of the server room, it is common for the fire door to be wedged open to allow for air to circulate.

There are 2 servers in the server room that run the following services:

- domain controller running dynamic host configuration protocol (DHCP) and domain name system (DNS) services, and file and printer services
- web server
- remote access services server (not functional)

All employees are issued desktop computers. Some accountants use their personal laptops to connect to the network through a bring your own device (BYOD) policy.

The meeting room has a single laptop that requires the accountants' credentials to sign in. It has been observed that most accountants will use a mixture of their own and their colleagues' details to sign in, dependant on the documents required for the meeting.

DoubleUp Bookkeeping are considering moving to Office 365 for their business. They currently use Google Docs and would like to explore how Office 365 could support collaboration and remote working.

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)

You have been provided with the following computers that are configured on the DoubleUp Bookkeeping network:

Server:

Computer name: **Serv01**

Username: **Administrator** Password: **Pa$$w0rd**

Reception desktop:

Computer name: **Desktop01**

Username: **reception** Password: **N/A (No password)**

Junior desktop:

Computer Name: **Desktop02**

Username: **IsaacA** Password: **Password**

Users:

The following user accounts are available to use throughout your work:

Users	Account	Password	Role
Charlie Mears	CharlieM	Pass	Owner
Jessica Smith	JessicaS	Finance	Accountant
Natalia Remy	NataliaR	Reception	Head Office Receptionist
Marco Shelvey	MarcoS	passworD	Company Partner
Isaac Ashton	IsaacA	Password	Junior
Noah Wilson	NoahW	birminghamcityFC2000	Junior

Groups:

Current documented Active Directory group membership:

Group	Members
Domain Admins	Charlie Mears
Staff	Jessica Smith, Marco Shelvey, Natalia Remy, Isaac Ashton, Noah Wilson

Instructions for students

With your experience within the IT sector, you are concerned at the number of security vulnerabilities observed. You ask the owner, Charlie, to complete a risk assessment document on the office and network infrastructure based on the information provided. Your company are trying to be compliant with the ISO27001 and want to ensure security is the best it can be.

You have been provided with a copy of the floor plan for the office and access to multiple machines on the network.

Perform a security risk assessment on the site and network, identifying any threats to company resources, data and security.

Recommend physical, administrative and technical controls and explain why these recommendations will improve physical and network security.

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 office floor plan and neighbouring buildings
- the security on the server
- the 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

The following evidence should be recorded in the workbook:

- 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)

DoubleUp Bookkeeping currently has a dated security policy in place. This was created in 2017 before the office merger.

You are concerned that because the current security policy was created in 2017, the network infrastructure is currently at risk and the likelihood of security threats will increase as the business grows. You are particularly concerned about the use of shared login details for the meeting room and weak password implementation.

You have asked to recommend security controls that must be implemented to protect the network infrastructure.

Instructions for students

To make the owner aware of your concerns, you are planning to deliver a report which will include the kinds of controls that should be included in a security policy to keep it updated. You should submit a report that includes recommendations for controls that could be included in a security policy.

Your presentation should include:

- administrative controls to be implemented and your reasons for choosing these controls
- technical controls, including hardware and software mechanisms
- 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

The following evidence should be recorded in the workbook:

- 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)

DoubleUp Bookkeeping partners are concerned about recent reports of theft within the area. They are concerned that in the event of equipment being stolen, this would not only impact their operations, but could breach General Data Protection Regulation (GDPR) legislation around the storage of financial documents.

There are currently no policies or procedures in place and no contingency planning has been undertaken with this issue in mind.

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 theft in a timely manner, whilst protecting systems and data.

The impact to end of year accounts means that operations must resume within 24 hours after any theft.

The business is willing to invest a substantial budget for this project. They do request that the server is maintained onsite due to the data it stores.

You should focus on recommendations that maintain business continuity and restore operations ahead of financial concerns.

You need to write:

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

You will have access to the following equipment:

- word processing software

Evidence required for submission to NCFE

The following evidence should be recorded in the workbook:

- 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

The managing director is impressed with your security proposal and has asked you to implement some of the security recommendations that you have made across your previous work on this project.

Using the computers provided, demonstrate how you can improve computer, network and data security for DoubleUp Bookkeeping.

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

Actions taken should include:

- suitable authentication should be implemented across the network
- appropriate encryption must be employed to secure data on mobile devices
- domain security policy should be reviewed and updated appropriately
- client and server operating systems must be configured to mitigate security issues
- user accounts should not be able to access data restricted to them

You should consider the following information: current systems configuration

Server

Operating system:

- Windows Server 2012 Standard Edition (with GUI)

Server roles:

- dynamic host configuration protocol (DHCP)
- domain name system (DNS)
- Active Directory domain control

Firewall:

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

Anti-virus:

- Windows Defender

Installed software:

- Home

Client build

Operating system:

- Windows 10

Firewall:

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

Anti-virus:

- Expired Norton 360

Installed software:

- Sage One installed on all desktop systems

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
- print screens 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

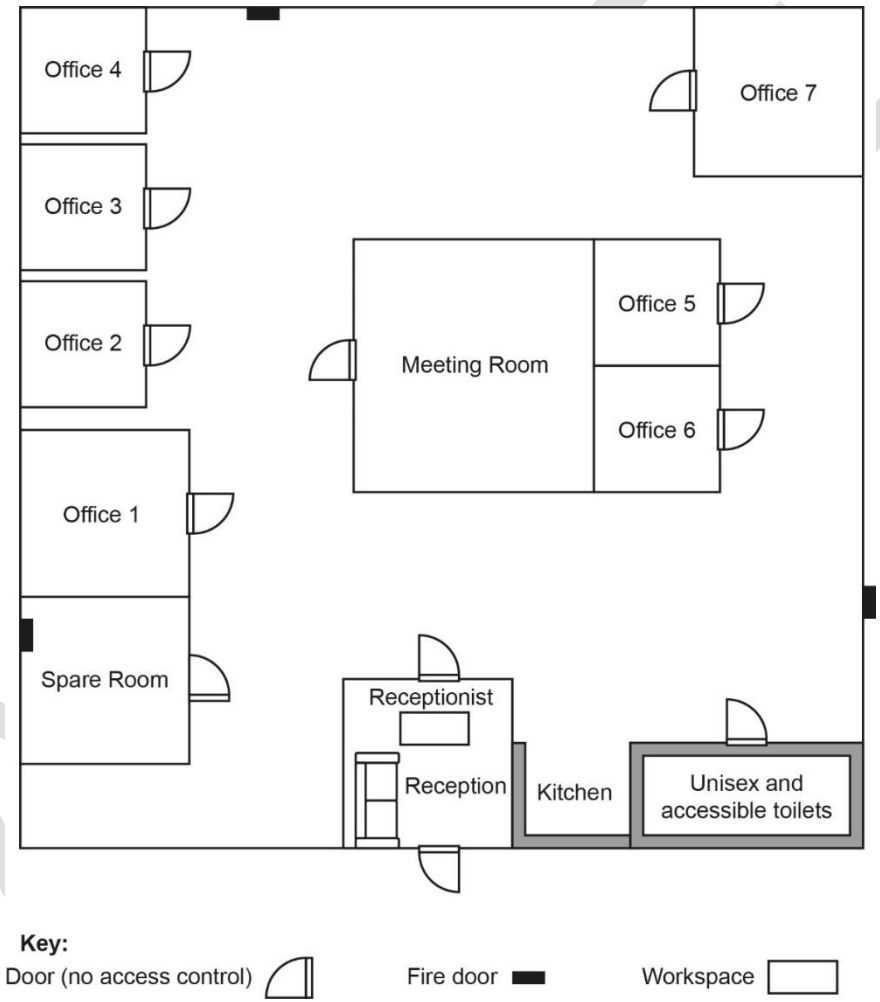
All print screens should be numbered and linked to the task as stated in the electronic workbook.

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 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

Office floor plan



Document information

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.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Additional sample material		01 September 2023
v1.1	Sample added as a watermark	November 2023	17 November 2023