T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 3

Assignment brief

v1.1: Specimen assessment materials
21 November 2023
603/6901/2

Internal reference: DSS-0013-05

NCFE

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

Cyber Security

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 allowed for all tasks.

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

Save your work regularly as you work through the assessment.

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

Electronic files should be named using the following format for identification purposes – Surname_Initial_student number_evidence reference, for example 'Smith_J_123456789_Task1'

Timing

You have 6 hours 30 minutes to complete all tasks within this assignment (including 30 minutes of reading time for you to familiarise yourselves with the additional supporting document – 'Company overview').

Task 1 = 2 hours 30 minutes (this will be completed in 1 session on day 1)

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

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

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: 70 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

(30 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (15 marks)

PO3: Discover, evaluate and apply reliable sources of knowledge (15 marks)

Task 2

(20 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (10 marks)

PO3: Discover, evaluate and apply reliable sources of knowledge (10 marks)

Task 3

(20 marks)

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data (10 marks)

PO2: Propose remediation advice for a security risk assessment (10 marks)

Scenario

Problem identified

The IT manager at Willow Technology has highlighted to management that there has been a rise in cyber-attacks and is concerned that future attacks could adversely affect the business. They are considering how well the business would cope if cyber-attack were to occur. They are concerned the business, as a new and expanding company, does not have all its policies or procedures in place yet to deal with this kind of emergency. The management team have highlighted that in the event of an incident the network and services would need to be operational within 3 days.

To help you complete this assignment, a breakdown of the current company infrastructure and security measures has been provided in the additional document ('Company overview'). You will need to refer to this document throughout the assignment and use this as a reference point for tasks 1 and 3.

Brief

In your role as a technician for Willow Technology, you have been asked by your manager to evaluate the site and current software programs in place, make recommendations to improve site and software security, and recommend actions for the company in order to deal with a cyber-attack incident.

Task 1: security risk assessment

Time limit

2 hours 30 minutes

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

Your manager has asked you to undertake a risk assessment and validate the company's network with regards to cyber security.

(30 marks)

Instructions for students

To help you complete this task a breakdown of the current company infrastructure and security measures has been provided in the additional document ('Company overview'). You will need to refer to this document throughout the task.

Your manager has asked you to evaluate the 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.

Using the provided risk assessment template, you should undertake your risk assessment.

You should consider:

- the information provided in the company overview document
- the security on the servers and computers
- security risks that could occur because of lack of auditing/monitoring
- prioritisation of the remediation actions
- potential Impact of damage
- RAG rate – low, medium or high rating

You will have access to the following:

- word processing software
- the internet risk assessment template (more lines can be added as required)

Evidence required for submission to NCFE

- completed risk assessment template

Task 2: security guidelines recommendations

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.

Willow Technology are a new and growing company and therefore requires guidance in identifying the security policies required to meet compliance and regulatory needs. Your manager has identified that the current information security policy document is generic and untested. They have asked you to consider what measures could be implemented to make this policy more secure and robust and write a report of recommendations.

(20 marks)

Instructions for students

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

Your report should include:

- a justification of the user and administrative controls to be implemented
- a description of how each control will be enforced within the business
- considerations of any frameworks, legislation, regulations or standards related to each control (where appropriate)
- justification for your recommendation for:
    - managing information security incidents
    - the security and protection of data
    - upgrading policies in line with business expansion
- full references for any online sources used

You will have access to the following:

- word processing software
- the internet

Evidence required for submission to NCFE

Report containing recommendations and justification for controls that could be included within the information security policy for Willow Technology.

Task 3: disaster recovery document

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.

Recently, there has been service outage due to denial of service (DoS) attacks near the site of the Willow Technology office. Your manager is concerned that further attacks 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, as a new and growing company, does not have all policies or procedures in place yet to deal with this kind of emergency.

(20 marks)

Instructions for students

To help you complete this task, a breakdown of the current company infrastructure and security measures has been provided in the additional document (‘Company overview’). You will need to refer to this document throughout the task.

Your manager has asked you to recommend a range of actions that could be taken to provide disaster recovery support from a service outage due to DoS attacks in a timely manner, whilst protecting systems and data. Your manager would like to have the business network recovered and fully operational within 3 days of a major disaster. The business is willing to invest a substantial budget of approximately £150,000 for this project, as it is estimated that an hour of downtime would cost the business £10,000 per year. You should focus on justifying recommendations that allow for disaster recovery and restoring operations ahead of concerns.

You need to write a disaster recovery document that includes:

- your recommendations in the case of service outages
- an explanation of how the actions you have taken will better protect the company

You will have access to the following:

- word processing software
- the internet

Evidence required for submission to NCFE

- disaster recovery document

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
							(further lines can be added as required)

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

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	Post approval, updated for publication		01 June 2023
v1.1	Sample added as a watermark	November 2023	21 November 2023