



# T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

## Digital Infrastructure

Assignment 3 – Pass

Guide standard exemplification materials

## T Level Technical Qualification in Digital Support Services Occupational specialism assessment

# Guide standard exemplification materials

## Digital Infrastructure

### Assignment 3

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>Task 1 .....</b>	<b>4</b>
<b>Task 2 .....</b>	<b>13</b>
<b>Task 3 .....</b>	<b>15</b>
<b>Task 4 .....</b>	<b>17</b>
Examiner commentary .....	28
Grade descriptors .....	29
<b>Document information .....</b>	<b>31</b>
Change History Record .....	31

## Introduction

The material within this document relates to the Digital Infrastructure occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

In assignment 3, the student must first analyse a penetration test of a network in order to identify any maintenance requirements. The second task requires the student to remotely carry out updates to the system.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

## Assignment 3

### 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

## Student evidence

### Risk assessment

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
1	Unauthorised access to whole network	Generic passwords	Files on the network  High	Everyone could have access to any logins due to using the same password, could lead to people accessing files they shouldn't have access to.  Critical	Everyone in the business knows everyone else's password so this is likely to happen.  High	This would be a risk if there was anyone trying to see things that they shouldn't.  High	Mandate user password changes at next logon and configure regular password changing with a complex requirement.	Technical/ administrative – preventative
2	Physical security of the server	No security to server cabinet	Company files	The server cabinet is in an open room that anyone within the organisation has access to, this means that should someone gain access to the building then they could easily get access to the server cabinet.  High	Someone would have to know exactly where the cabinet was, and this cabinet may have a small lock on as they do as standard.  Medium	Should someone get access to this then they could damage or destroy the data, or even steal the server.  High	In an ideal world this cabinet would be locked in a small room with no access to a window (see diagram for suggestion) which would make the machine physically safer.	Physical/ technical – corrective

3	Unauthorised access	Lack of physical security in the car park	Access to property	Anyone could get access to the outside of the building, making the interior significantly less secure.  Medium	Should someone want to access the building they would then be able to do some of the other things identified within this table.  Medium	They would gain access to the computers and could potentially access content or steal the devices.  Medium	I would recommend the installation of a fence around the car park to minimise the access to the building, this would ensure that the building would become more secure.	Physical – preventative
4	No monitoring	Lack of CCTV System	Access to property	Without a security camera system, should something happen then it could be impossible to investigate what happened or who was involved.  Critical	This is currently a certainty, and a critical security issue.  Critical	People could get access to the office; CCTV would be a deterrent and also a feature to allow investigation.  Low	The installation of a CCTV system which can be remotely monitored and recorded would allow for both a deterrent and investigation tool.	Physical/ technical – deterrent/ detective
5	No audit history	Lack of access monitoring system	Access to property	There's no sign in or sign out book so no one knows if anyone is in the building or not.  Critical	At the moment people have free access to all rooms and the building itself, this could lead to anyone having access at all times.  Critical	Anyone having access to any room at any time makes it difficult to restrict access to the likes of the server room.  High	The installation of ID badge access on each door would ensure that only people that should have access will be able to enter.	Physical/ technical – preventative/ detective



6	Physical security of laptops	Lack of security at hot desks	Physical devices	Should someone gain access to the hot desks at a quiet time then they could steal a device or access any files left open.  Medium	This would mean someone accessing the open plan office and not being noticed by anyone else, whilst possible the chances are lower.  Low	Should someone manage to get access to the computer then they could steal the device.  Medium	The installation of Kensington locks in the hot desk area would ensure that users could secure their devices whilst they are in the office. The update of the company policy to ensure that these are used and signage to remind users would support this.	Physical/ administrative – deterrent
7	No audit history, physical security	No policies	Access to equipment and files	Due to no policies – everyone is completing things differently and independently.  Critical	This is happening now.  Critical	With no policies around passwords, security, or retention this means that some people are keeping things longer than they should.	Introduction of several policies would ensure that everyone is operating to the same high level of security and this should prevent many situations.	Administrative – corrective/ directive
8	Unauthorised access to files	No security on shared files	Company files	Anyone can access all files and folders across all the different computers, meaning there is little privacy, including access to HR and Payroll.  Critical	Currently everyone has access to all data.  Critical	This means that not only does everyone have the ability to access everyone's data they could also delete it if they wanted to.  Critical	With immediate effect each folder should be restricted using policies to only allow each department to access their own files.	Technical – corrective

9	Lost/stolen machine could lead to stolen files	No encryption on local machines	Company files	Currently should a laptop be lost or stolen then the files could be readily accessed by someone who was able to bypass the password.  High	This would only become an issue should someone either misplace or have their laptop stolen.  Medium	The risk is potentially access to various different levels of company data dependent upon what the user had saved upon the machine.  High	The installation of Windows 10 Pro and the activation of Bitlocker would ensure that should the device be lost or stolen then people would be unlikely to be able to access the data.	Technical – preventative.
10	Stolen server could lead to stolen files	No encryption on server	Company files	Should the server be stolen, which is possible with the current security set up, then someone could potentially access the data very easily. Included with the lack of backup – this could close the company.  Critical	This could be a problem with the current set up as there is no security to protect the server and it is in a room with a window and a door to hide it from the main office.  High	This could lead to access to the data should the server be stolen as it would be possible for someone to bypass the login password and access the data.  High	The activation of Bitlocker would ensure that the data would be protected should someone steal the server and not have access to the encryption password.	Technical – preventative
11	Hardware failure/theft/loss could lead to lost files	No file backup	Company files	Should there be any technical failures, or stolen equipment then there is no backup of data to restore from.  Critical	Hasn't happened yet; but could do.  Critical	This could lead to data loss either on a small or large scale depending upon the machine that was lost/failed.  Critical	It would be a priority to implement a backup solution.	Technical – preventative

12	Unauthorised access to data	Extended period before password required on screensaver	Company files	Potentially there could be unauthorised access to the data if someone walked away from their computer and didn't lock it.  Medium	This would depend on whether people regularly forget to lock their computers.  Medium	This could lead to a security breach of data or in extreme cases data deletion.  High	With the introduction of policies within the company, group policies should also be altered to ensure that screens lock automatically after a set period (for example 3 minutes).	Administrative/technical – preventative
----	-----------------------------	---	---------------	---	---	---	---	---

Risk levels: Low, medium, high, critical	Business control types: Physical, administrative, technical	Mitigating control types: Preventative, detective, corrective, deterrent, directive, compensating, acceptance
---	--	--

### 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

### Student evidence

#### Security policy report

Password policy

Here should be a combination of group policy and HR policy to ensure the security of passwords.

Group policy – minimum complexity of passwords, regular changing of passwords (for example 90 Days), password history.

HR policy – no writing down of passwords, no sharing of passwords.

Physical access policy

This is required to ensure that the building is kept secure, this should include ensuring that ID badges are worn throughout the time as the brief states that there is regularly new faces. There should also be policies around no tailgating when entering the premises.

### Screen locking

This should be a combination of group policy and HR policy to ensure that data is kept secure. This will support ensuring that the company follows General Data Protection Regulations (GDPR).

Group policy – screens should be set to go to screensaver after a set period (for example 5 mins) in case someone walks away from their computer and does not lock it.

HR policy – people should be required not to leave their screen without locking them, as this could breach GDPR.

### Clean desk policy

In order to protect customer and company data people should be able to ensure that there is no data left out on desks if there isn't someone sat there, this would mean that there would have to be a secure location to keep, such as lockable drawers or lockers.

### Training policy

There is a requirement for all staff members to ensure that they complete regular training regarding data security, health and safety, and physical and mental wellbeing – this should include phishing training to protect the data and logins.

This phishing security training should then be tested on a regular basis to ensure that users do not release data such as logons easily. These could support the OWASP principles of working safely online.

### Software policies

There should be policies in place around regular updates, these updates could be pushed out centrally to ensure that everyone is kept up to date and software updates which include security updates could be enforced and reduce vulnerabilities.

## 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

### Student evidence

#### Business continuity recommendations document

In the event of a flood we need to ensure that the business is able to keep working while the office is closed. We need to have plans to keep working if the server is damaged by the flood and staff can access resources.

My first recommendation would be to implement a remote working system and use something similar to Citrix so that the team could have full access to their computer no matter whether they were working. This would allow users to work from home while the office is closed.

An online storage solution for files could be implemented – such as SharePoint to ensure that everyone can access the team files regardless of their location. SharePoint is cloud based meaning we will not be keeping critical data onsite. In the event of a flood staff can keep working accessing the data and continue to work.

A policy should be created that ensures that everyone knows what will happen in the situation where access to the office is restricted. This should also include an emergency call tree to ensure that everyone knows what has happened and what the plans are.

For the business to perform best should the office not be available, it is important that the IT team have an accurate asset database so that they are aware of who has what equipment. This will also include if people have access to broadband.

They could ensure that they have access to another office where they could get together to work from if the office was not available.

## **Disaster recovery recommendations document**

In order to ensure that the business can recover from a flood the following need to be considered:

Backup solution – one needs to be implemented as soon as possible, this should be an off-premises solution due to the previous history of flooding, in an ideal world this would be a continuous online backup as flooding can often happen with very short notice and at any point in the day.

Whilst having a backup solution is important, the restoration needs to be tested regularly to ensure that the backup has worked successfully and will be able to be restored should the worst happen. This will also support in identifying how long it will take to restore should they need to.

Backups should include a basic disk image including all the configurations and settings applied as well as core software such as antivirus.

In the event of flooding damaging the server we will need a plan for what hardware and data to be restored first. We must assume a flood will write off our current server so we will need to:

- priority order a replacement server
- redeploy the server base image
- update the software with any patches to ensure the software is up to date
- recover data from backups to the server

Part of the policy needs to specify the roles that IT staff will take so that people know what it is that they have to do in order to recover from a disaster.



## 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.

## Student evidence

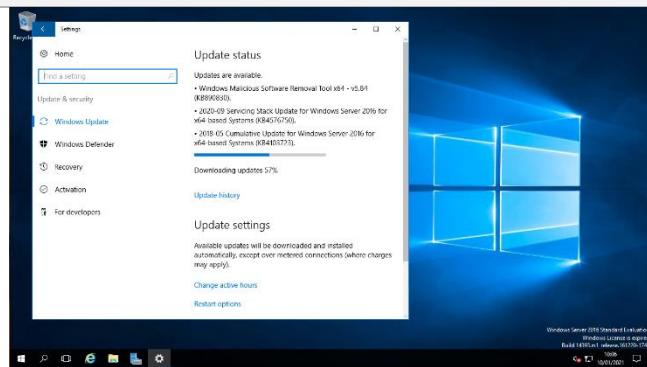
Please duplicate action 1 for each additional action you have taken to harden the system.

### Action 1

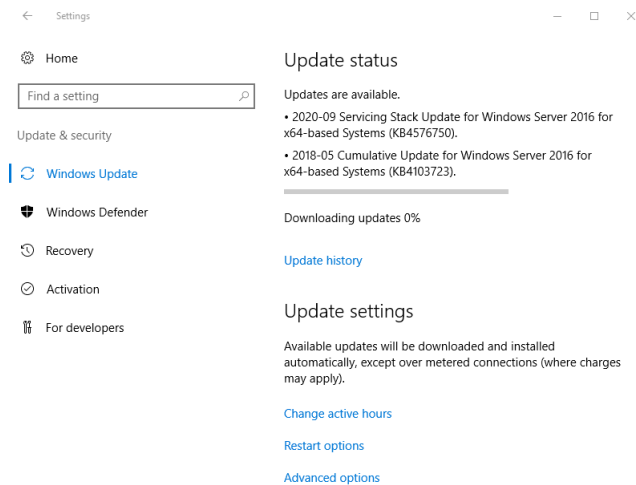
**Description of action you have chosen to implement:**

**Windows updates are required, running updates.**

**Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):**



**Those updates completed, and further ones were installed, more cumulative updates (includes security):**



**Any unexpected results found whilst hardening the system:**

None

**Explain how the action you have taken will better protect the system**

These updates are focused around security patches, and also included above is definition files for the Windows Malicious Software Removal Tool – Windows Defender.

**Websites accessed**

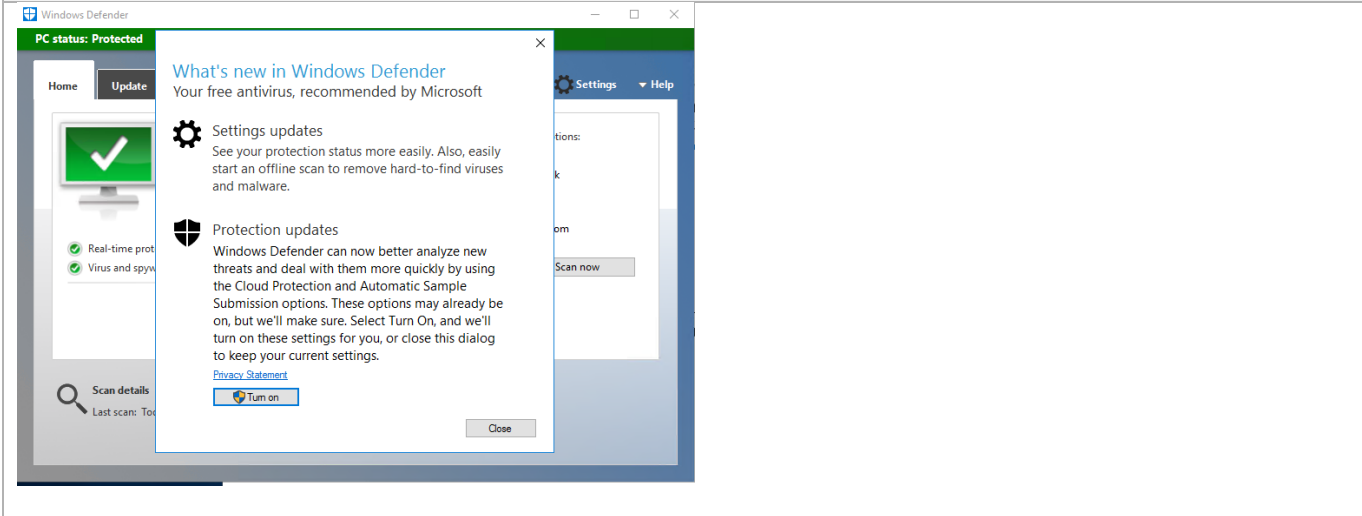
None – Accessed via the settings panel of Windows server.

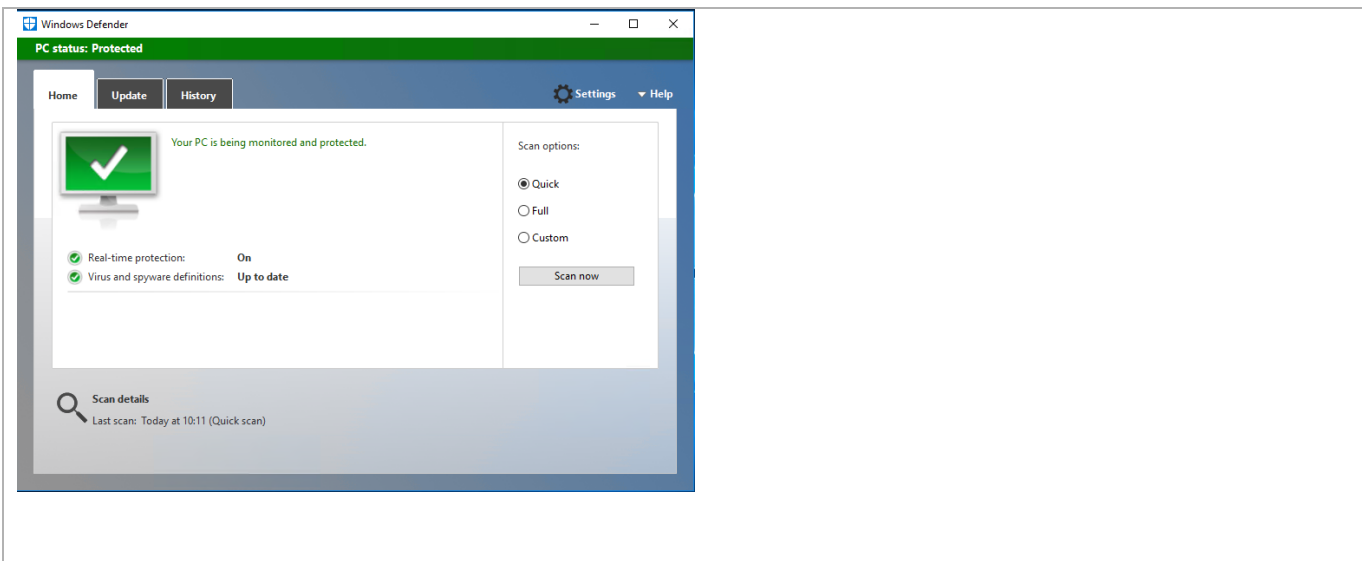
## Action 2

**Description of action you have chosen to implement:**

Windows Defender seems to have been disabled, this is an included anti-virus and anti-malware software which should be turned on unless something else is installed – which it does not appear to be. Whilst I am activating this I will also run a quick scan to check for any malicious software.

**Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):**





**Any unexpected results found whilst hardening the system:**

**None, nothing found on scan.**

**Explain how the action you have taken will better protect the system**

**Antivirus and anti-malware software ensures that the computer is less likely to be infected by any software that could affect the system or the data.**

**Websites accessed**

**None**

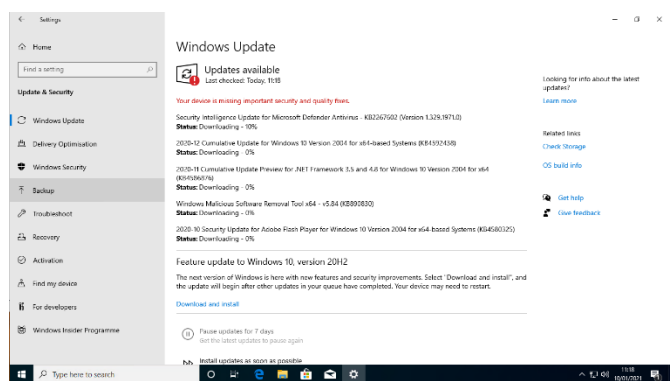
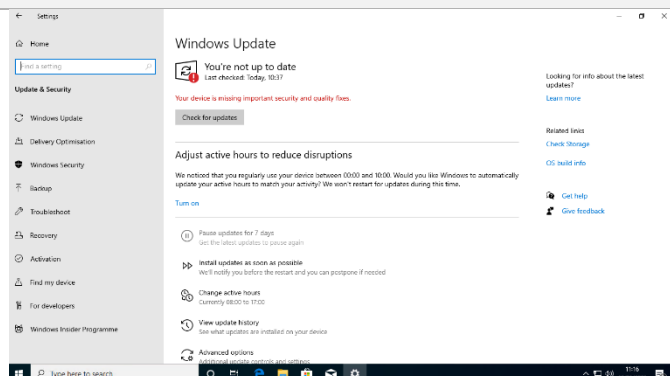
### **Action 3**

**Description of action you have chosen to implement:**

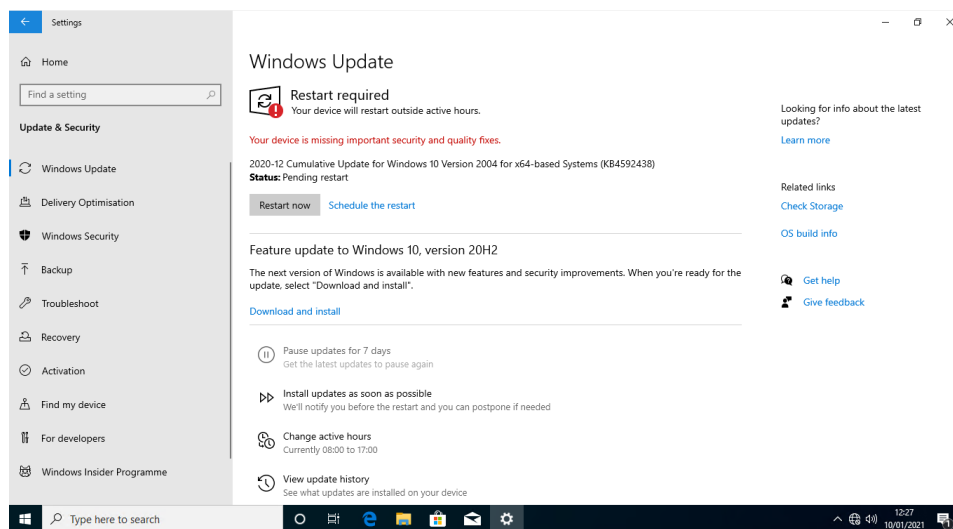
**Windows updates checked to ensure that the computer contains all the latest security updates – this will also include the latest Windows Defender definitions to ensure the desktop is as secure as possible.**

**Windows itself has identified that there are missing important security and quality fixes**

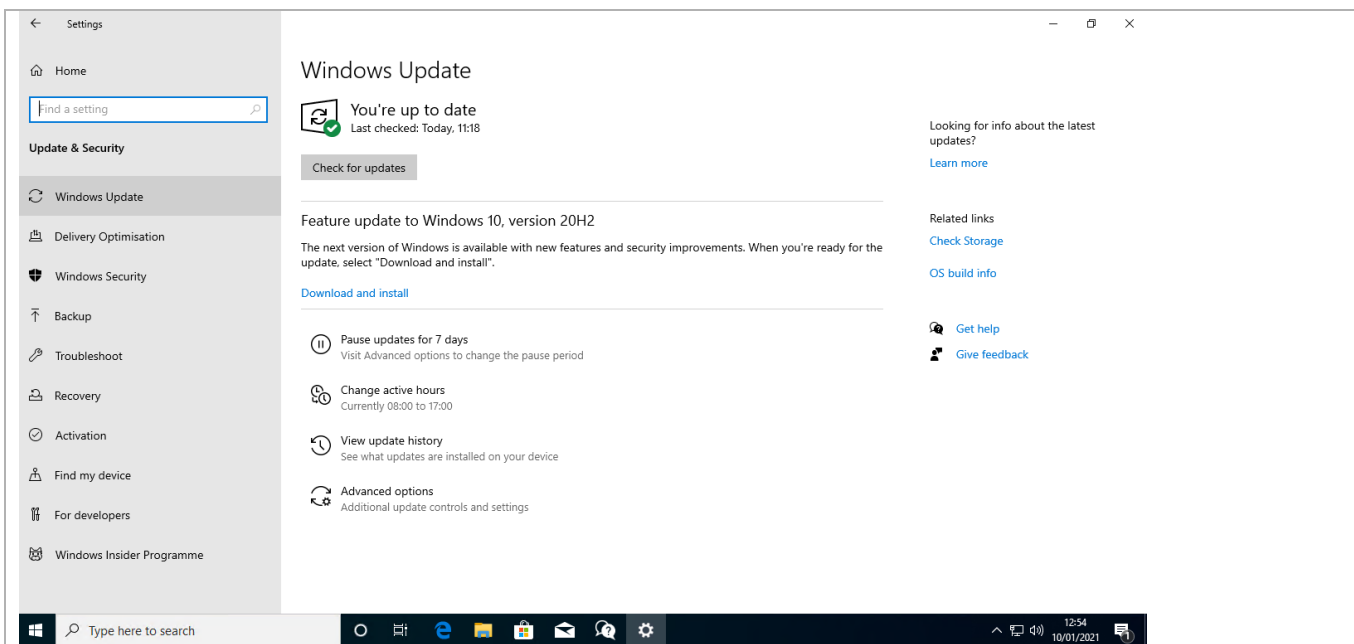
## Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):



## Windows is now installing various updates, including the Defender antivirus updates and the Windows Malicious Software Removal Tool.



## Fully up to date:



The screenshot shows the Windows Settings application, specifically the Windows Update page. The left sidebar shows 'Update & Security' selected, with 'Windows Update' highlighted. The main content area displays 'You're up to date' with a green checkmark icon and 'Last checked: Today, 11:18'. Below this is a 'Check for updates' button. A feature update to Windows 10, version 20H2 is announced, with a 'Download and install' link. A list of update options is provided: 'Pause updates for 7 days', 'Change active hours', 'View update history', and 'Advanced options'. On the right, there are links for 'Learn more', 'Check Storage', 'OS build info', 'Get help', and 'Give feedback'. The taskbar at the bottom shows the search bar and various application icons, with the system tray displaying the time as 12:54 on 10/01/2021.

**The machine was restarted as required by the updates.**

**Any unexpected results found whilst hardening the system:**

None

**Explain how the action you have taken will better protect the system**

As well as the updated security patches having the latest virus definitions will ensure that the machine has taken all precautions towards any malicious intentions.

**Websites accessed**

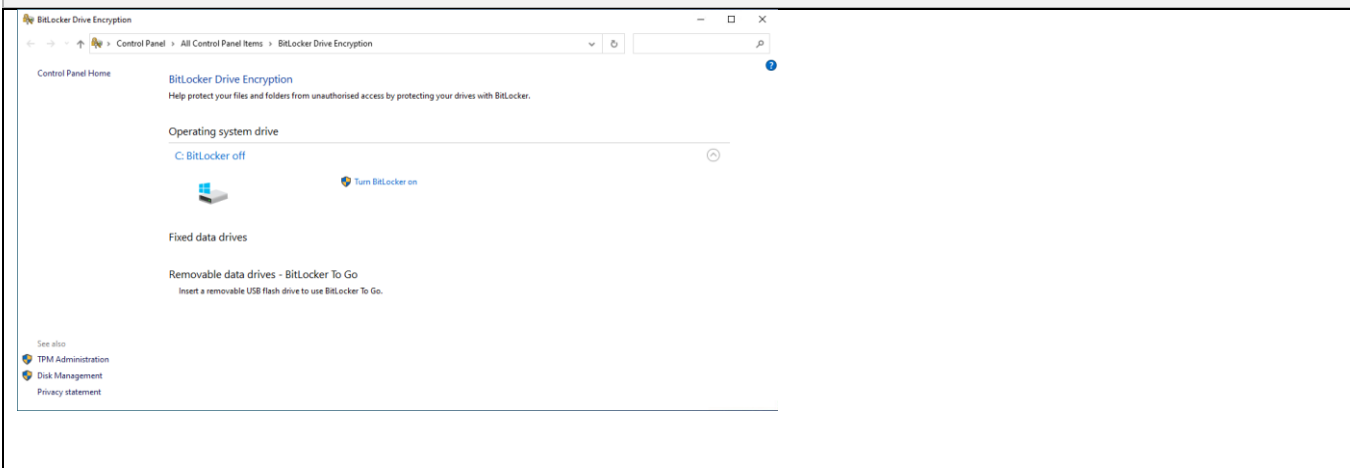
None

#### Action 4

**Description of action you have chosen to implement:**

Activate BitLocker to protect files should something happen to the desktop/laptop. This will prevent access to the files should the laptop be lost or stolen.

**Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):**



**Any unexpected results found whilst hardening the system:**

Unfortunately, I was unable to activate this on the virtual machine due to the lack of a TPM in the virtual machine, however on a live machine I could activate this.

I would also be able to activate Bitlocker to go on any devices that were being used to transfer data.

**Explain how the action you have taken will better protect the system**

Bitlocker would ensure that the storage of the computer would be as protected as possible should something happen to the computer (lost/stolen).

**Websites accessed**

None

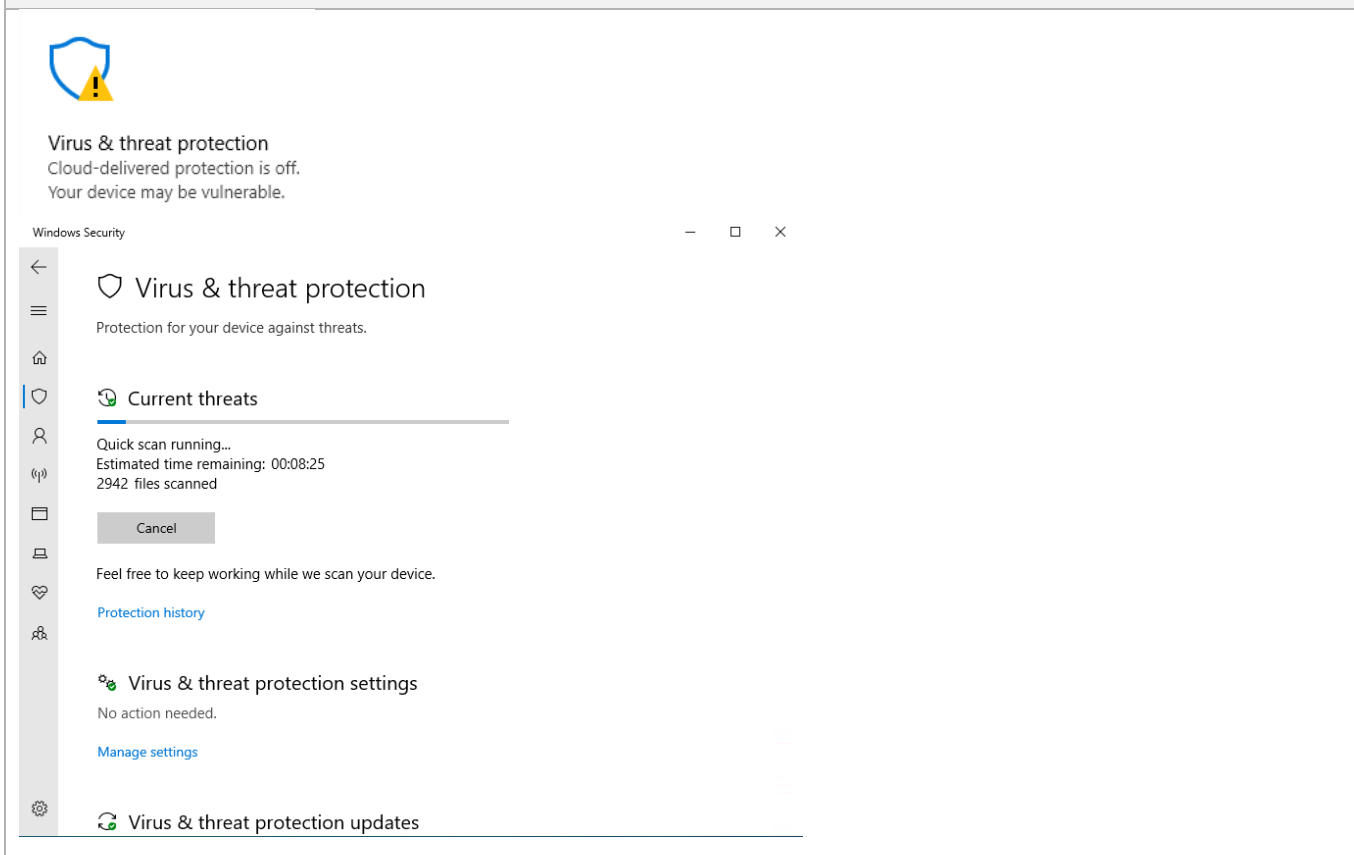
**Action 5**

**Description of action you have chosen to implement:**

Windows Defender Scan



**Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):**



**Any unexpected results found whilst hardening the system:**

None

**Explain how the action you have taken will better protect the system**

This will give the best attempt at checking that the system is kept clear of viruses.

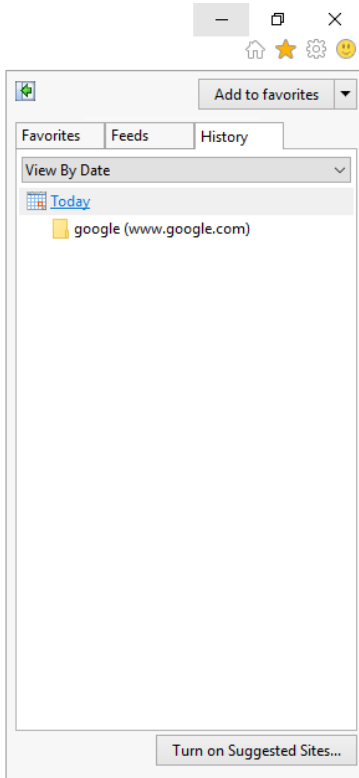
**Websites accessed**

None

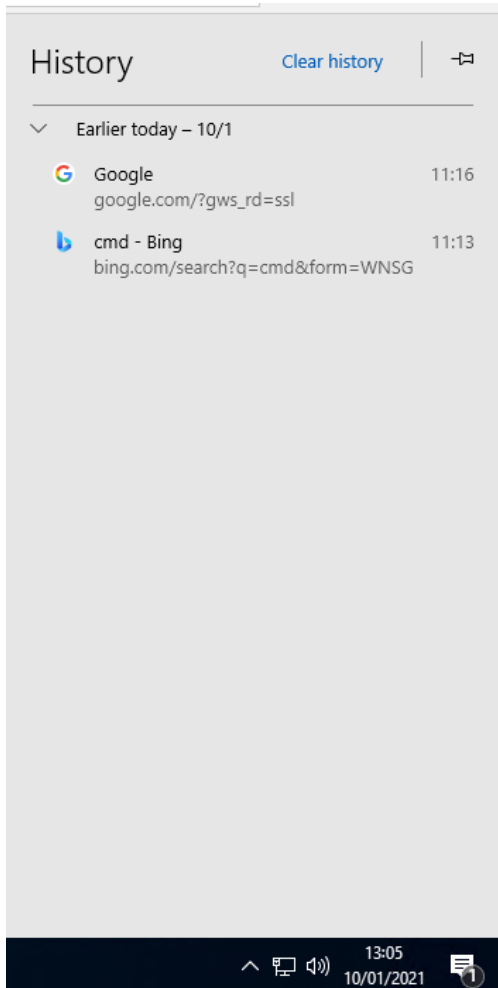
## Browser history

Please insert a screenshot of your browser history here.

### Server internet history



## Desktop internet history



## Examiner commentary

The student has achieved the grade for the following reasons:

The student demonstrated an understanding of the different risks across the organisation and identified risks in different areas of the business – physical, technical and administrative. The student has identified some suitable controls that should minimise the weaknesses identified. There were some other weaknesses that could have been identified within this assignment.

The student has identified some good recommendations that covers the requirements that were identified within the brief. They have identified some security controls that do indeed support the needs of the business; however, they have missed some other areas such as data security and were unable to link these to the full range of different legislations.

The student has written 2 reports that do indeed look at disaster recovery and business continuity, and these would be effective, however, they had missed some elements around the people and ensuring that the people know what they are doing. The 2 documents would ensure that the business could be up and running as quickly as possible.

The student has taken steps to mitigate the risks associated within the scenario. They have not differentiated much between the server and the client, although the actions would have been the same on both. They have managed to explain what they have done and why, but not been able to relate them to the scenario. They have added in basic protection for the machines and servers using the built-in tools that Windows provides. To demonstrate sufficiency for a higher grade, they would be expected to select a range of protection tools from different sources.

## Grade descriptors

The performance outcomes form the basis of the overall grading descriptors for pass and distinction grades.

These grading descriptors have been developed to reflect the appropriate level of demand for students of other level 3 qualifications, the threshold competence requirements of the role and have been validated with employers within the sector to describe achievement appropriate to the role.

Grade	Demonstration of attainment
Pass	The evidence showing installations and configuration setup is logical and displays sufficient knowledge in response to the demands of the brief.
	The student makes some use of relevant knowledge and understanding of implementing network infrastructure but demonstrates adequate understanding of perspectives or approaches associated with industry standards in digital infrastructure roles.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their implementations and configurations.
	The student is able to identify some information from appropriate sources and apply the appropriate information/appraise relevancy of information and can combine information to make some decisions.
	The student makes sufficient judgements/takes appropriate action/seek clarification with guidance and is able to make adequate progress towards prioritising and solving non-routine problems in real life situations.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques to plan, install, configure, deploy and populate network infrastructure and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to attempt to prioritise and solve problems with some attempt at verifying their implementations.
Distinction	The evidence is precise, logical showing installations, configuration and deployment that provides a detailed and informative response to the demands of the brief.
	The student makes extensive use of relevant knowledge and has extensive understanding of the practices of the sector and demonstrates a depth of understanding a threshold competency of the different perspectives/approaches associated with installing, testing, monitoring and maintaining digital infrastructure.
	The student makes decisive use of facts/theories/approaches/concepts, demonstrating extensive breadth and depth of knowledge and understanding and selects highly appropriate skills/techniques/methods to apply network infrastructure practices.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can

	combine information to make coherent decisions.
	The student makes well-founded judgements/takes appropriate action/seek clarification and guidance and is able to use that to reflect on real life situations in a digital infrastructure role; being able to apply implementation and configuration of the network.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in a digital infrastructure role and precisely applies this across a variety of contexts and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.
	The student can thoroughly examine data/information in context and apply appropriate analysis in confirming or refuting conclusions and carrying out further work to justify and evaluate strategies for solving problems, giving concise explanations for their reasoning.

\* 'Threshold competence' refers to a level of competence that:

- signifies that a student is well placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the TQ in a classroom-based setting (for example, in the classroom, workshops, simulated working and (where appropriate) supervised working environments)
- signifies that a student has achieved the level for a pass in relation to the relevant occupational specialism component

## U grades

If a student is not successful in reaching the minimum threshold for the core and/or occupational specialism component, they will be issued with a U grade.

## Document information

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2020-2023.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

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.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of 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	Published final version.		May 2021
v1.1	NCFE rebrand		September 2021
v2.0	Annual review 2023: Amends to grade descriptors to ensure clarity	June 2023	19 June 2023