T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 3 - Distinction

Guide standard exemplification materials

v1.1: Specimen assessment materials
September 2021
603/6901/2

Internal reference: DSS-GSEM-03

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment

Guide standard exemplification materials

Digital Infrastructure

Assignment 3

Contents

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, lack of audit history	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 and there would be no history of who accessed or made changes. 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, delete things that they didn't want people to see or if someone managed to discover a user's password. High	Mandate user password changes at next logon and configure regular password changing with a complex requirement.	Technical/ administrative - preventative
2	Hacking of the network	Standard administrator username	Full network High	Hackers attempt to use the default "administrator" due to it normally being available on a machine, having to guess the username makes the network significantly more secure.	Hacking is happening 24/7 and as there is a wide range of open services due to remote working access to the server. High	If someone was successfully able to hack into the server then they would have access to all materials stored on this. They would be able to access all files and	Disable administrator account, ensuring that different accounts have administrator security privileges.	Technical/ administrative - preventative

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
				High		services. High		
3	Unintended administrative privileges could lead to security weaknesses	Using everyday logins as admin accounts	Full network	Should a user be performing everyday tasks whilst running as an administrator, they may be able to delete sensitive files, or install malicious software without intention. Critical	This is happening currently. Critical	Malicious software could be installed accidentally and potentially put the entire network at risk. Critical	Ensure that administrators have two accounts, their regular day to day account and their own administrator account with higher privileges that would ensure they can still access administrator functions.	Technical/ administrative - corrective
4	Unauthorised access to the building	Lack of security entering building from car park	Physical equipment	Due to the access to the office being unprotected anyone could access the building at any time. They could access an unlocked computer or steal the physical computers. High	Due to no security this could happen at any time. Also due to no external security. High	Physical theft of equipment is a real possibility if someone entered during a quiet time (such as lunchtime) where the office might be quiet or unoccupied. High	Removal of entrance door from car park. This could be moved to enter from reception, meaning that it would be easier to ensure that reception was manned at all times. I would also recommend the installation of an access card lock system on the doors into the main office, which will be covered shortly.	Physical - corrective

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
5	Lone working/ unauthorised access	Lack of visibility of reception from office	Staff/ physical equipment	This could give access to the reception whilst no one is watching, and they could have access to the computer or steal the computer. High	Due to no monitoring, or visibility, this is a potential problem at any time. High	No one would be aware if someone entered the reception area whilst it was unmanned. High	Whilst having an open reception is a necessity the addition of a window to reception would help make the building more secure, ensuring that this is manned at all time – either receptionist or security team member.	Physical - compensating
6	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 this 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. However, this could lead to overheating and an air conditioning unit would be required. This room will also require physical security, such as access card security.	Physical/ technical - corrective
7	Unauthorised access	Lack of physical security in the car park	Access to property	Anyone could get access to	Should someone	They would gain access	I would recommend the	Physical - preventative

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
				the outside of the building, making the interior significantly less secure. Medium	want to access the building they would then be able to do some of the other things identified within this table. Medium	to the computers and could potentially access content or steal the devices. Medium	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.	
8	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	This is not a direct risk in itself, the risk is the other things identified, 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
9	No audit history	Lack of access monitoring system	Access to property	Currently there is no monitoring of anyone entering or exiting the building, or rooms within the building. ID Badge access panels	At the moment people have free access to all rooms and the building itself, this could lead to anyone having	Anyone having access to any room at any time makes it difficult to restrict access to the likes of the server room, or again	The installation of ID badge access on each door would ensure that only people that should have access will be able to enter. This would ensure that only authorised people can enter	Physical/ technical – preventative/ detective

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
				on each doorway would monitor who accesses which rooms and also prevent access to unauthorised people. Critical	access at all times. Critical	investigate should something happen. High	each room, such as the IT office, or the server room.	
10	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 either steal the device or access the data. 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
11	Physical security, no audit history	Lack of security on fire exit near server room	Server equipment	Someone currently could gain access to the room that the server is in without anyone being aware, also allows for someone to exit the server room	Due to the closed room with the server room in having no one able to see it would mean that this could be a big risk. High	Without any security/alarm people could access the fire exit, which currently is unmonitored and could have unlimited access	An alarm on the fire exit which sounds each time the door is open would ensure that this could not be used as a quick exit or entrance for anyone.	Physical - deterrent

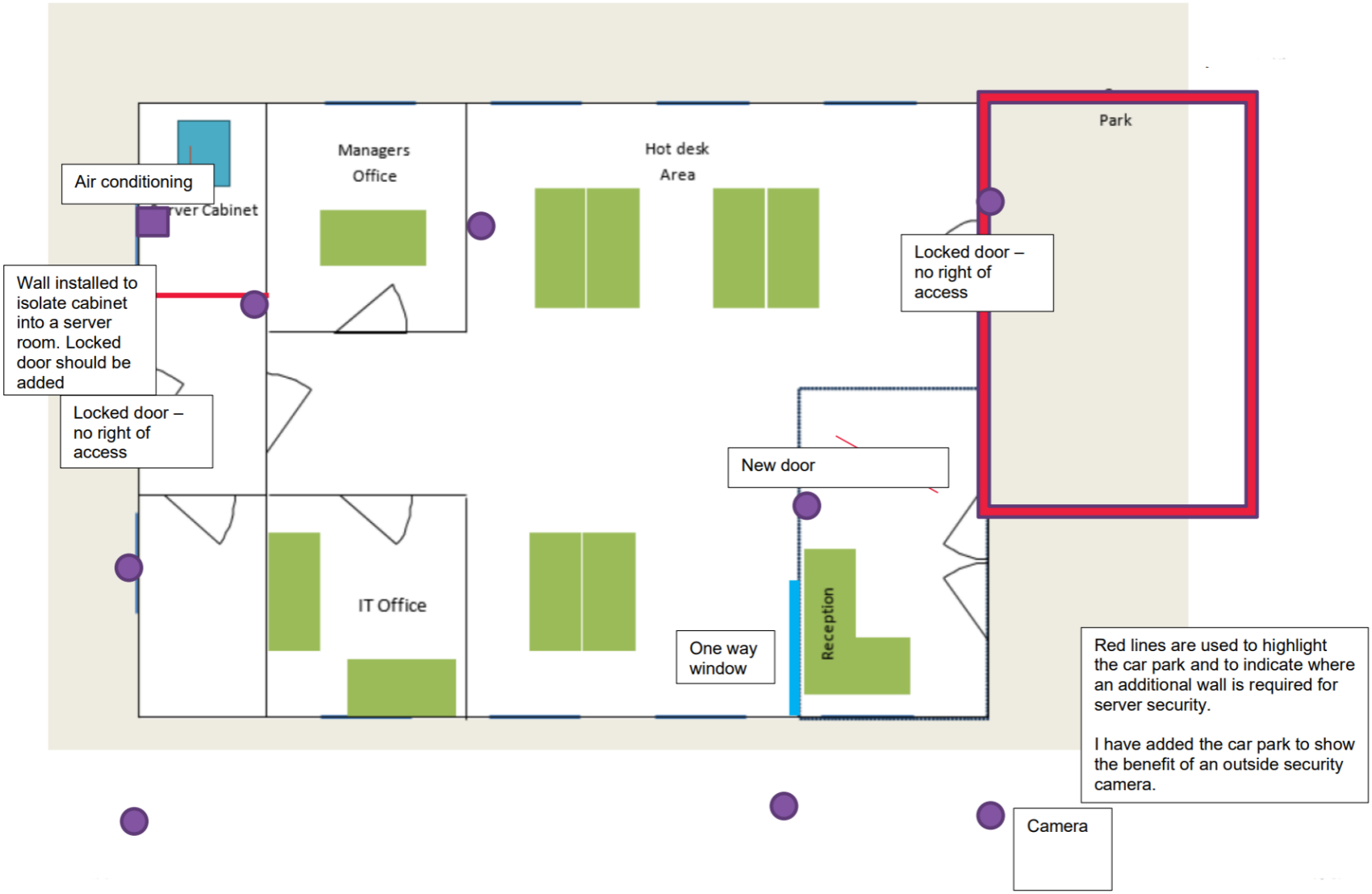
#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
				unnoticed. High		should the door be left open. High		
12	No audit history, physical security	No policies	Access to equipment and files	Due to no policies – everyone is completing things differently and independently. Critical	This is happening now. Critical	With no policies around passwords, security, or retention policies this means that some people are keeping things longer than they should, some people may be destroying things early.	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
13	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 or make copies of this data should they wish. Critical	With immediate effect each folder should be restricted using policies to only allow each department to access their own files. Each user could be allocated their own storage space to prevent access to anyone being able to view or delete.	Technical - corrective
14	Lost/stolen	No encryption on local	Company	Currently	This would	The risk is	The installation of	Technical –

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
	machine could lead to stolen files	machines	files	should a laptop be lost or stolen then the files could be readily accessed by someone who was able to bypass the password. High	only become an issue should someone either misplace or have their laptop stolen. Medium	potentially access to various different levels of company data dependant upon what the user had saved upon the machine. These users will include sales people. High	Windows 10 Pro and the activation of BitLocker (with recovery IDs saved at head office) would ensure that should the device be lost or stolen then people would be unlikely to be able to access the data.	preventative
15	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 setup 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 setup 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
16	Hardware failure/theft/loss could lead to lost	No file backup	Company files	Should there be any technical	Currently this appears not to have been	This could lead to data loss either on	It would be a priority to implement a	Technical - preventative

#	Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Action	Control type
	files.			failures, or stolen equipment then there is no backup of data to restore from. Critical	an issue however this could lead to a significant loss of data. Critical	a small or large scale depending upon the machine that was lost/failed. Critical	backup solution, ideally to an online platform that allows continuous backup – for example OneDrive for individual users. For the server platform there would need to be the implementation of a backup solution that allowed the data to be kept offsite and safe from Malware.	
17	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 (eg 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


Air conditioning
Server Cabinet
Wall installed to isolate cabinet into a server room. Locked door should be added
Locked door – no right of access
Managers Office
Hot desk Area
Park
Locked door – no right of access
New door
IT Office
One way window
Reception
Red lines are used to highlight the car park and to indicate where an additional wall is required for server security.
I have added the car park to show the benefit of an outside security camera.
Camera

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

There should be a combination of group policy and HR policy to ensure the security of passwords. Password policies are important for security and aid with compliance with standards such as ISO 27001. Whilst it is easy to implement an electronic control (passwords) it is important to follow this up with an administrative control to ensure that users follow password security rules. Most cyber attacks start with an unnecessary leak of password or similar so the HR policy as an administrative control will give teeth to enforce compliance as action can then be taken against users treating their passwords without respect and sharing them inappropriately.

Controls recommended:

- 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 are regularly new faces. There should also be policies around no tailgating when entering the premises. Tailgating is allowing others to enter the building with you on your ID card – human nature means that we tend towards trust and politeness allowing an attacker to bluff their way onsite easily.

Again, increasing the level of security here will aid with ISO 27001 compliance.

Controls recommended:

- staff ID cards to be worn at all times
- no tailgating policy for all staff

Screen locking

A very simple solution and a widely occurring problem is related to users walking away from their computer and leaving the screen unlocked. This is a risk as it allows an attacker to maliciously access the network on the user's machine undetected. This 'lunchtime attack' is a serious risk but can be fixed easily. By using a combination of group policy and HR policy to ensure that data is kept secure. This will support ensuring that the company follows GDPR (General Data Protection Regulations).

Controls recommended:

- group policy – screens should be set to go to screensaver after a set period (such as 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
- using someone's computer maliciously without permission would be an example of breach of the Computer Misuse Act

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 these in, such as lockable drawers or lockers. A good clean desk policy protects in a couple of ways. Firstly it means that sensitive or personal data will not be left on display accidentally (GDPR compliance) and also prevents paper being left cluttered including potentially on or near computers/fan vents creating a fire risk (health and safety)

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 cannot access resources.

Ultimately, regardless of the reason – be it flooding or other situations that require people to suddenly not have access to the office.

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

The solution should include the use of Citrix or Azure based virtualised desktops. This would allow the team to access through a software client on their personal computer as if they were logged in to a company computer. This will give the team full access to their desktop no matter whether they were working within the office, or on the road. This would support the general working of the office and also ensure that business continuity should continue regardless of whatever happens to the office, with no downtime. To implement this we need to understand whether staff do have access to computers at home they can and are willing to use for work purposes.

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 access the data and continue to work. SharePoint is an effective collaborative tool and will keep company data securely in the cloud. This will mean the risk to our data is minimal at all times and there will effectively be no drop in service keeping staff working.

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 include a flowchart that explains the steps to be taken and how things should be at each stage. This should also include an emergency call tree to ensure that everyone knows what has happened and what the plans are.

In order 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 and if there are any areas where there may need to be equipment issued for the duration of the emergency. This will also include if people have access to broadband, or they require mobile 4G dongles to allow for remote working.

In an ideal situation there will be a plan for a remote working location where people could get together to continue working together, this could be within a client/partner's site or a remote location that had been deemed suitable in advance.

With the site out of action we still need to ensure that equipment on site is protected. Although damaged, a server and its hard drives could still be stolen and date recovered from them by the attacker. Part of the continuity plan needs therefore to identify staff with the task of entering the premises as soon as it is deemed safe by the authorities with the task of retrieving key hardware and relocating it to a secondary location. By using a failover site like this we can ensure that we always have servers in place and working.

By implementing these business continuity recommendations, in the event of flood (or other disaster) the business is ready and can adapt its working practice with no effective loss of service to our customers.

Between the disaster recovery plan and the business continuity plan this should ensure that the business can continue as quickly as possible.

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.

I would recommend using a cloud backup solution as this will mean that we back data up remotely and securely to our cloud provider so that we do not have the data onsite and at risk.

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.

Part of the recovery process will involve sourcing replacement equipment. It would be prudent to have identified the vendor and equipment we would require and review this regularly so we can order replacements efficiently. Once on site we can recover the server quickly from the disk image but restoring data can be a lengthy process, particularly if the data is on the cloud. It would be good practice therefore to identify a ‘restore to’ date, with only data that has been edited or created after that date being restored. The theory is that data older than 3 months is not likely to be accessed day to day and by restoring this smaller amount of data we can be up and running quickly. If a request for a file or data older than the restore to date is needed, this can still be requested and recovered by IT from the backups.

In order to ensure that disaster recovery is done as quickly as possible there should be a flowchart created in order to ensure that the process could be as easy as possible. This should have identified flows and test points to make sure that everything has been followed to ensure the smooth restoration of business, this would include utilising the emergency call tree (to inform people) and then follow the business continuity plan (as below).

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

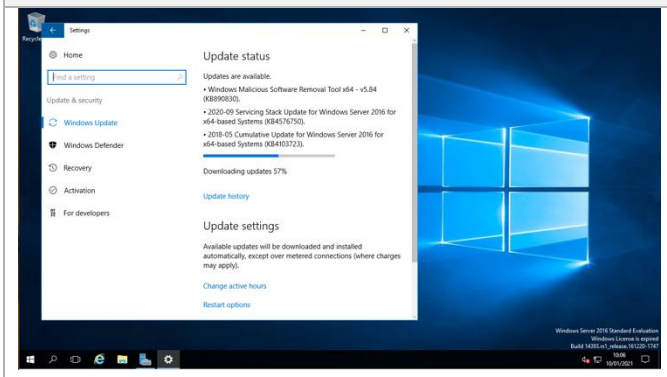
Student evidence

Please duplicate ‘Action 1’ for each additional action you have taken to harden the system

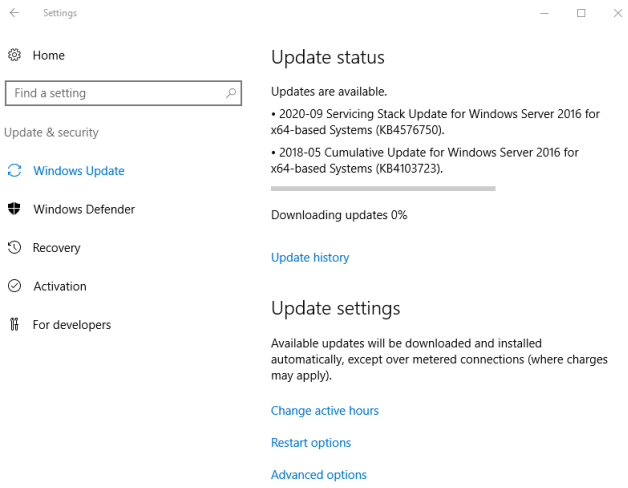
Action 1

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

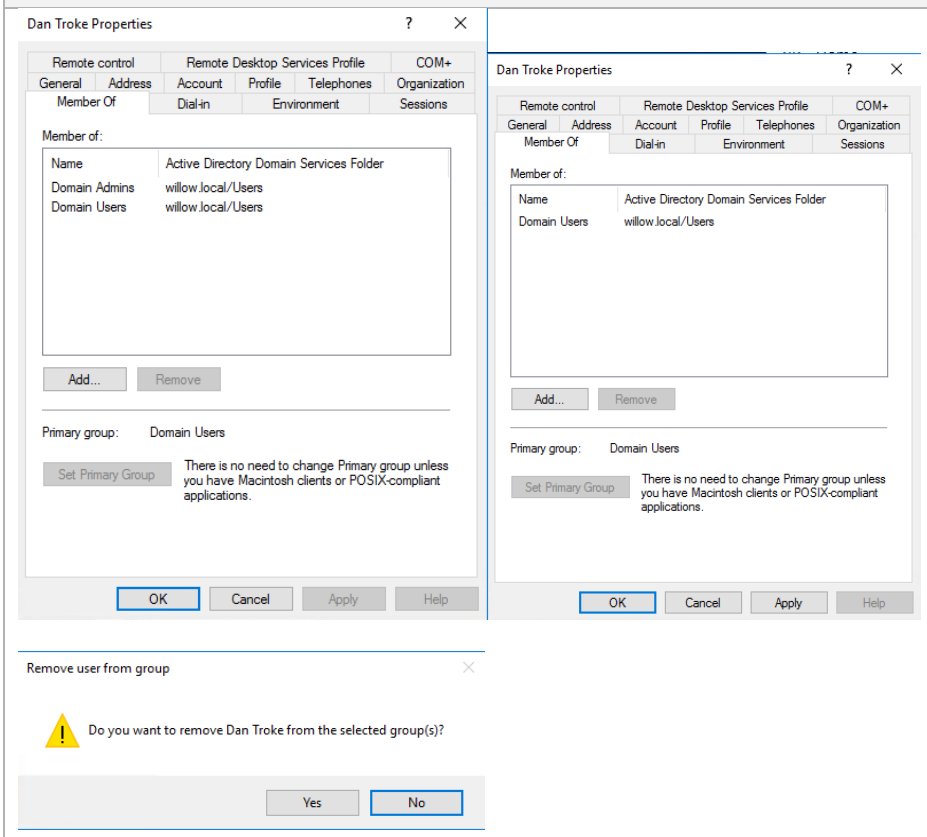
Explain how the action you have taken will better protect the system
These updates focus around security patches, and also included above is definition files for the Windows Malicious Software Removal Tool – Windows Defender, keeping these up to date will ensure that the machine is as protected as possible.

Websites accessed
None – accessed via the Settings panel of Windows server.

Action 2

Description of action you have chosen to implement:
Removal of Dan Troke's administrator privileges, as a sales director he has no reason to be an administrator.

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 ensure that only people who should be able to access everything, and install software, should have this administrator access.

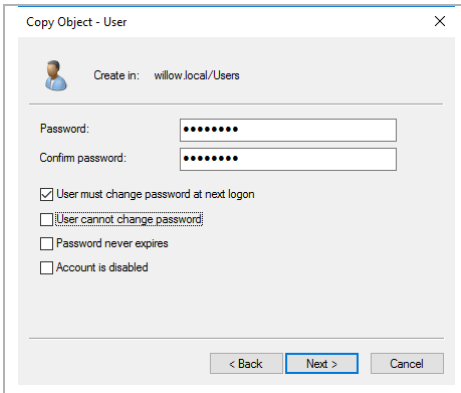
Websites accessed

None – managed through AD users and computers.

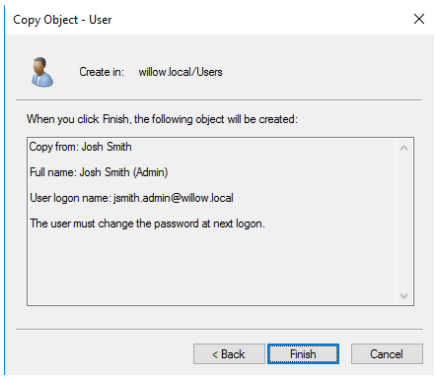
Action 3

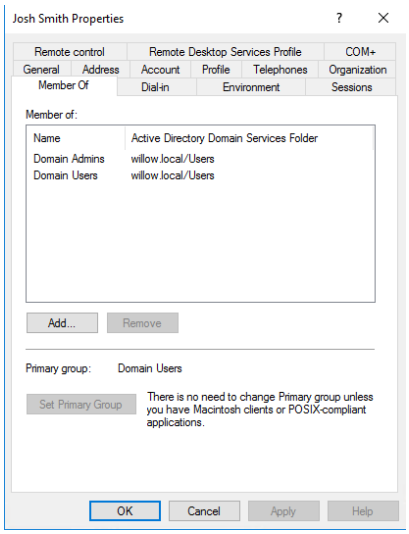
Description of action you have chosen to implement:
Creation of new admin account for Josh Smith, then removal of admin group from his account.

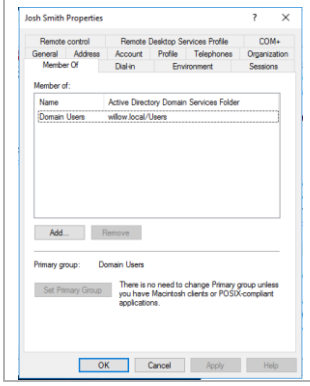
Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):



Set with the same password he uses currently but with the requirement to change passwords at next logon.







Any unexpected results found whilst hardening the system:
None

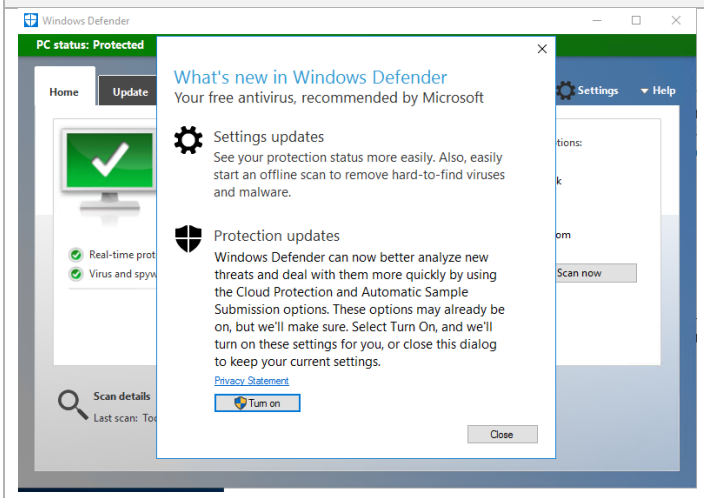
Explain how the action you have taken will better protect the system
By ensuring that Josh does not use an administrator account for his daily logon then he is much less likely to install something by accident or have his administrator account breached.

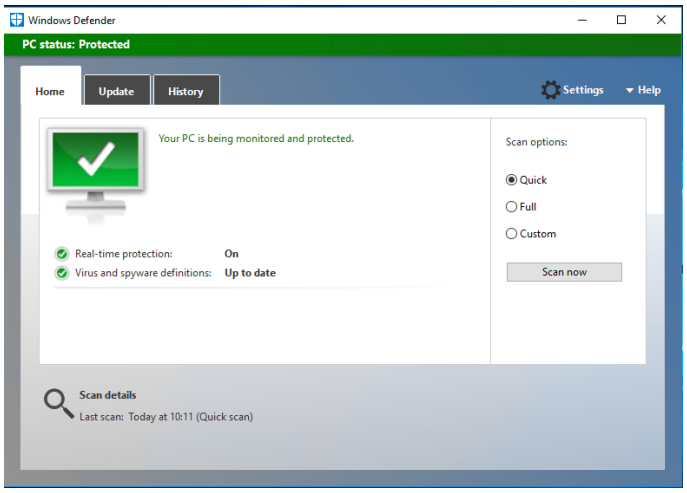
Websites accessed
None – managed through AD users and computers.

Action 4

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 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

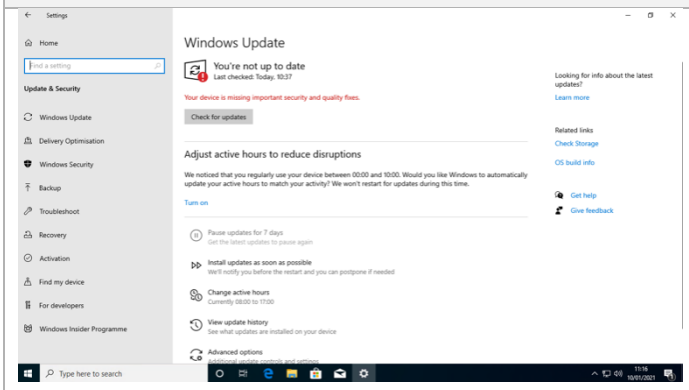
Antivirus and Anti-Malware software ensures that the computer is less likely to be infected by any software that could affect the system or the data.

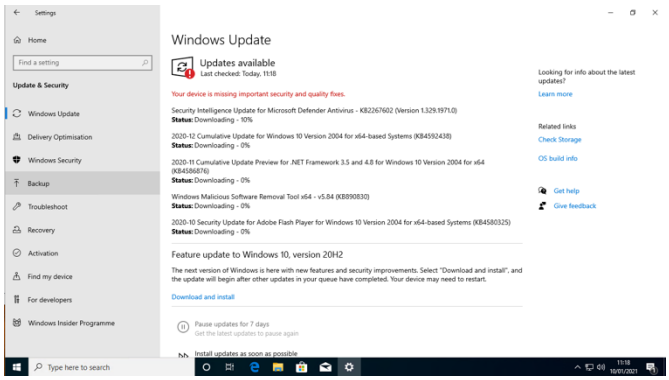
Websites accessed
None

Action 5

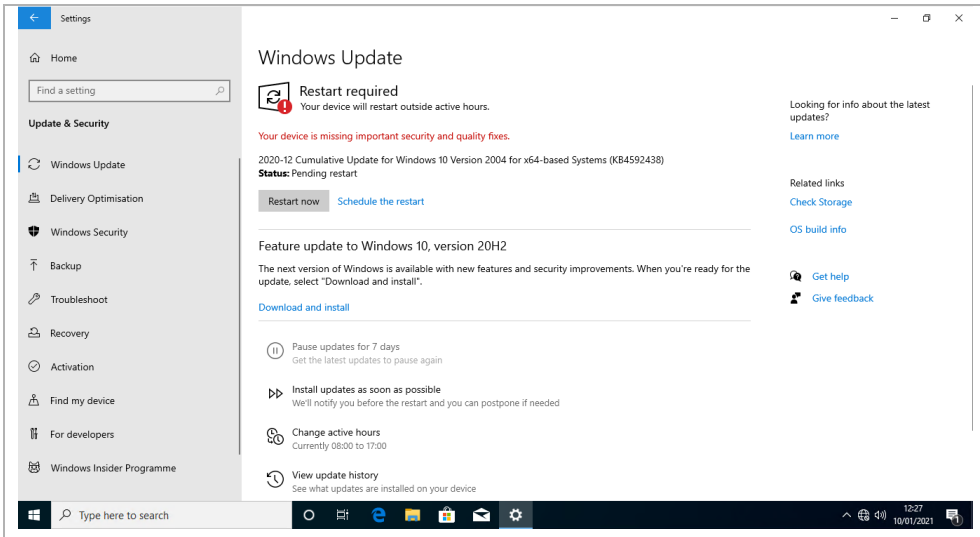
Description of action you have chosen to implement:
Windows updates checked to ensure that the computer contains all the latest security updates – this will also include the latest Windows Defender definitions to ensure the desktop is as secure as possible. **Windows itself has identified that there 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):

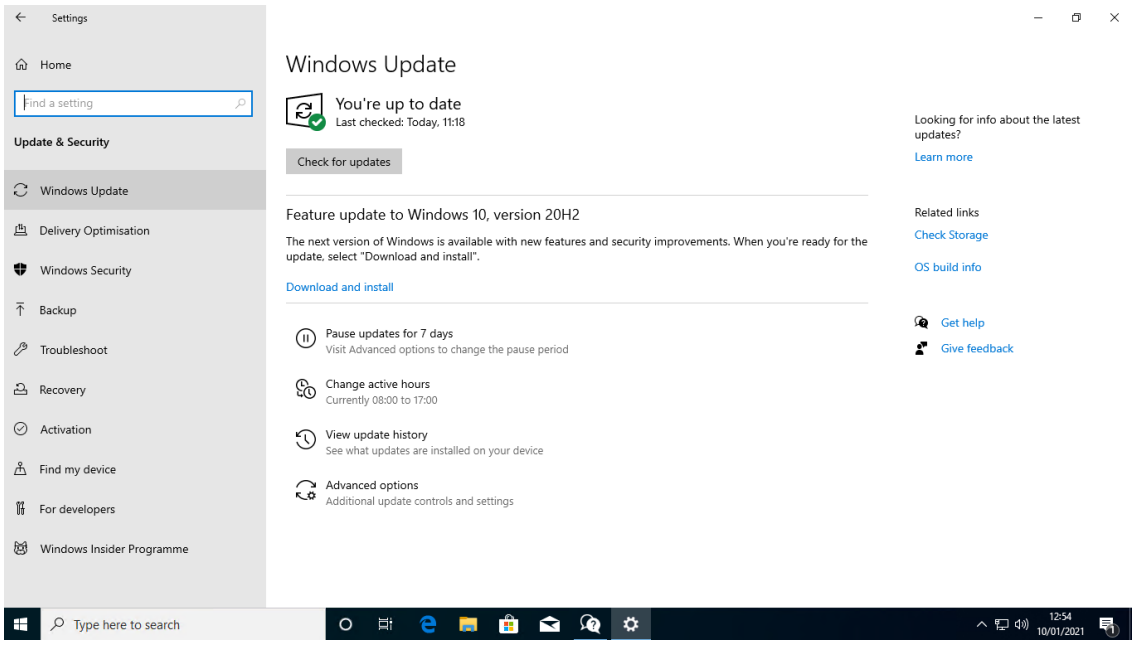




Windows is now installing various updates, including the Defender Antivirus updates and the Windows Malicious Software Removal Tool.



Fully up to date:



The machine was restarted as required by the updates.

Any unexpected results found whilst hardening the system:
None

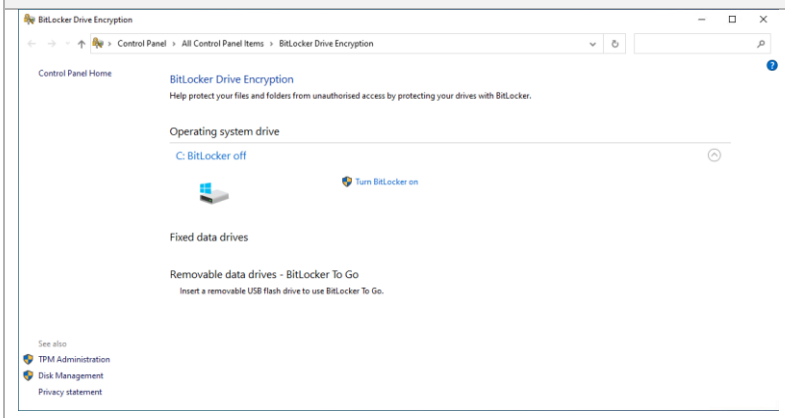
Explain how the action you have taken will better protect the system
As well as the updated security patches, having the latest virus definitions will ensure that the machine has taken all precautions towards any malicious intentions.

Websites accessed
None

Action 6

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.

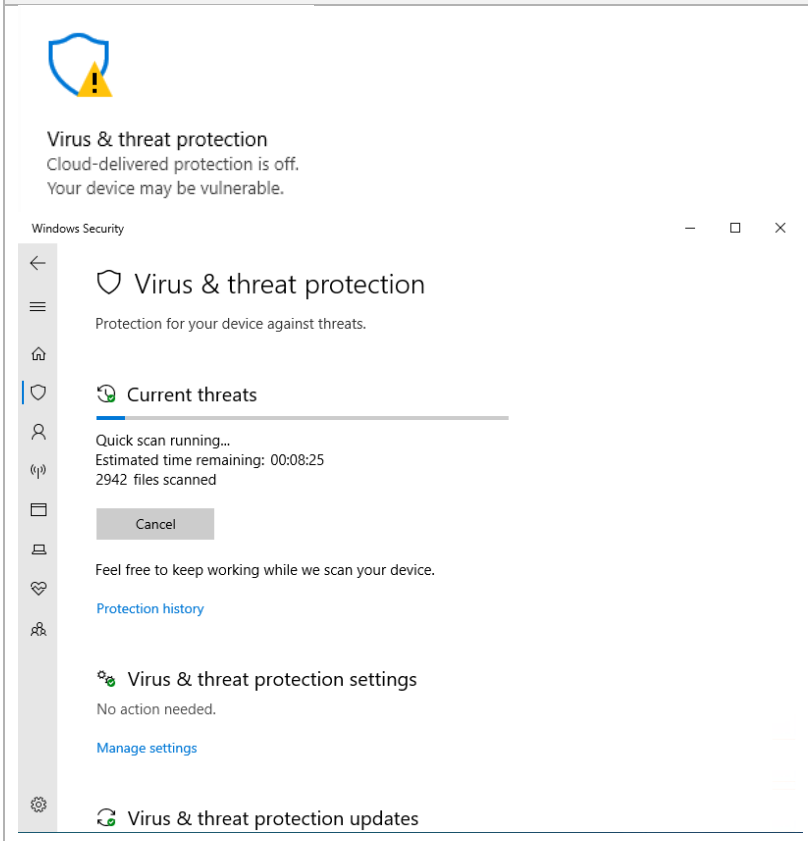
Explain how the action you have taken will better protect the system
BitLocker would ensure that the storage of the computer would be as protected as possible should something happen to the computer (lost/stolen).

Websites accessed
None

Action 7

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

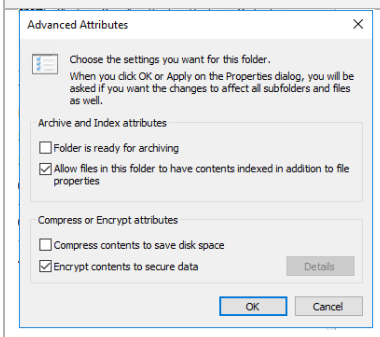
Explain how the action you have taken will better protect the system
This will give the best attempt at checking that the system is kept clear of viruses and malicious software to keep the system running at its best and also protecting the data on the machine.

Websites accessed
None

Action 8

Description of action you have chosen to implement:
EFS (Encryption) added for finance folder to protect data

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

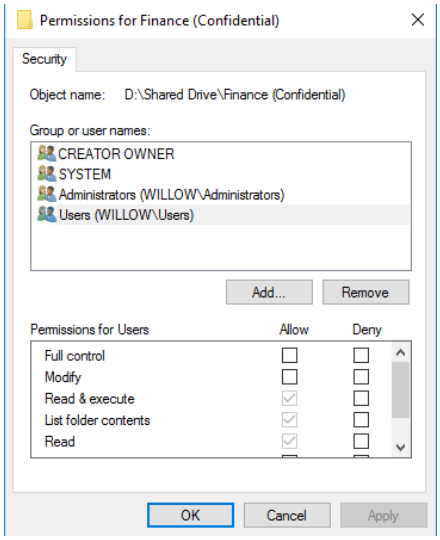
Explain how the action you have taken will better protect the system
This will add to the security to ensure that should someone gain access to the server that they will find it difficult to access the sensitive documentation stored in this folder.

Websites accessed
None

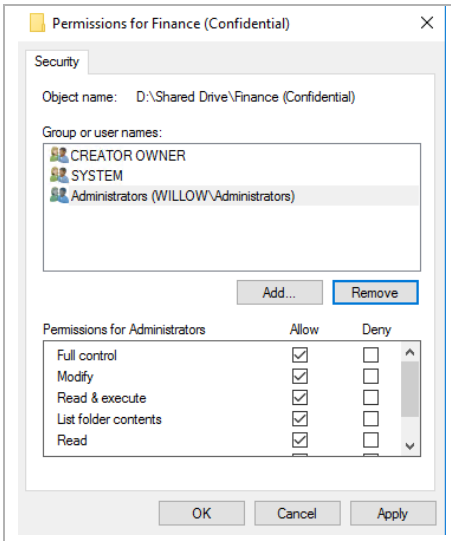
Action 9

Description of action you have chosen to implement:
File sharing restricted on shared drive

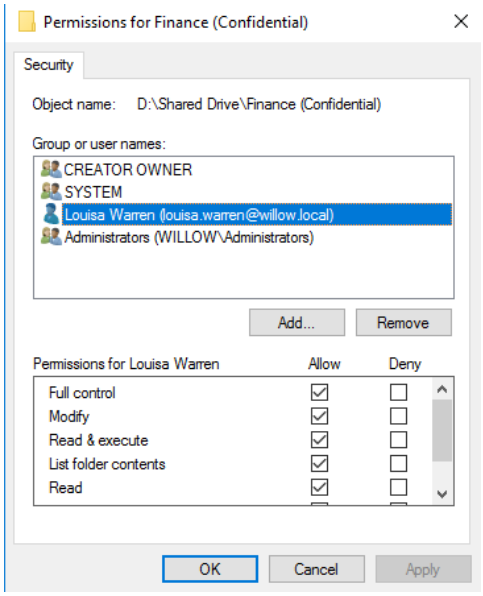
Screenshots of server and/or client settings before the configuration change, during the change and after the change (the reconfigured system):



Users Group removed.



Added the finance team member to be able to access this folder.



Louisa and the admin are now the only people that can access this folder.

Any unexpected results found whilst hardening the system:
Permissions were set to inherited, this had to be disabled before specific access could be set.

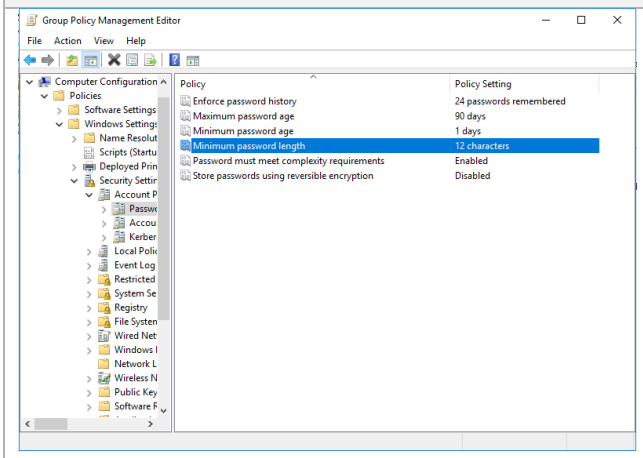
Explain how the action you have taken will better protect the system
This will protect the data from being accessed by people that shouldn't be – for example this folder may contain the details of everyone's wages which should not be accessible to anyone except finance.

Websites accessed
None

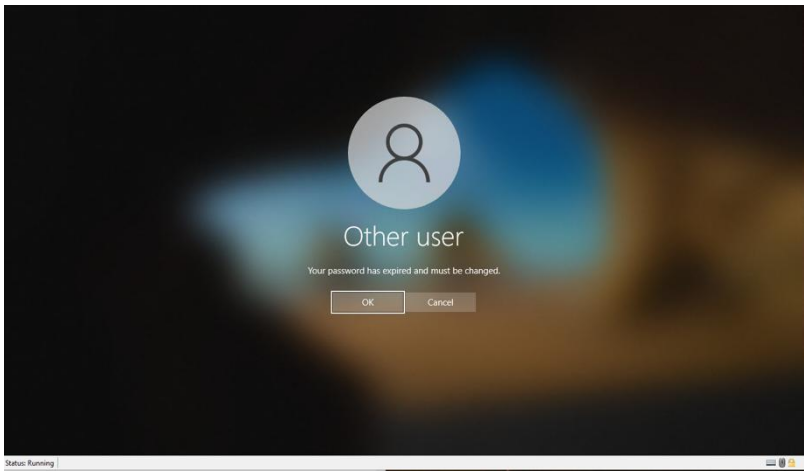
Action 10

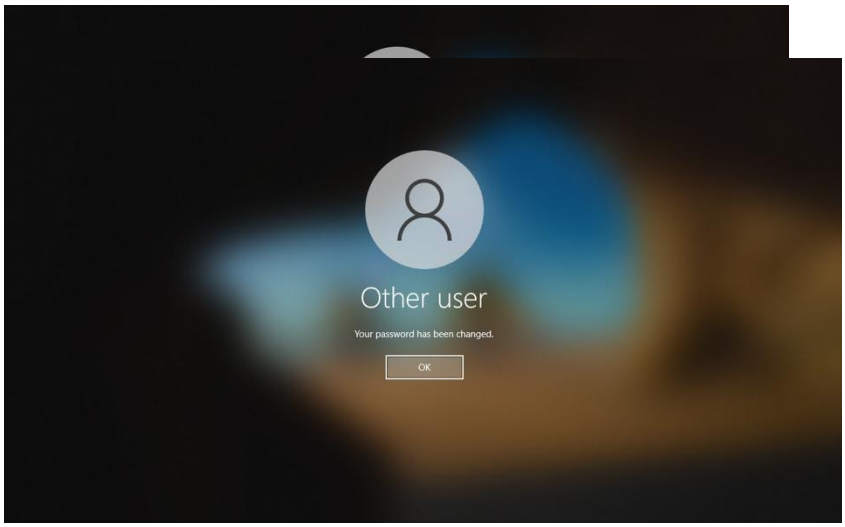
Description of action you have chosen to implement:
Password complexities mandated on the server.

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



This meant that when Bonnie next logged on she was forced to change her password:





Any unexpected results found whilst hardening the system:
None

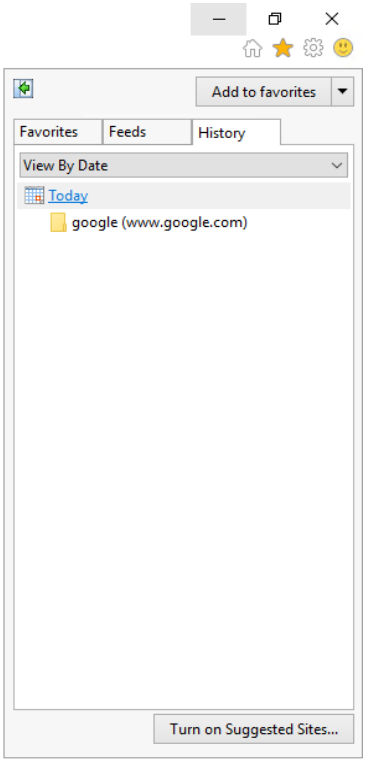
Explain how the action you have taken will better protect the system
This will ensure that people don't have passwords recorded, should they be compromised then they will be changed at regular intervals

Websites accessed
None

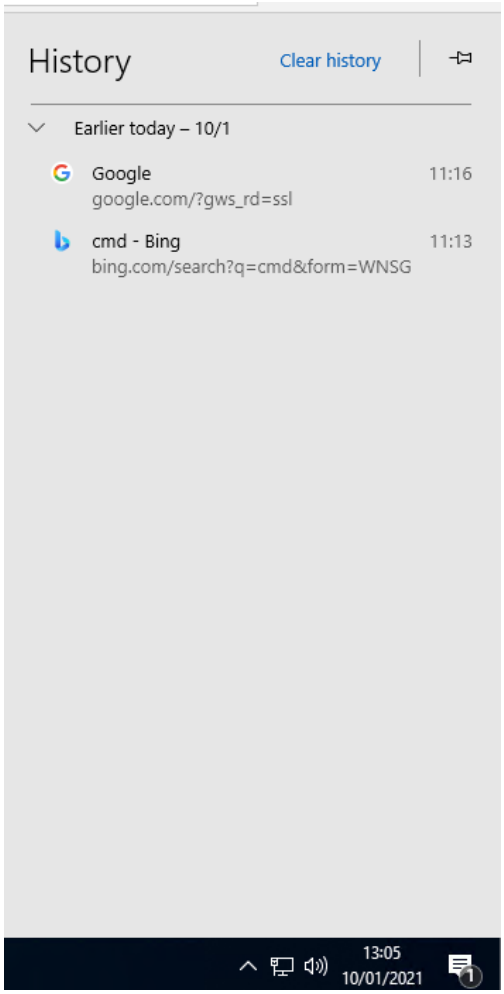
Browser history

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 excellent understanding of the different risks across the whole organisation and identified risks in all areas of the business – physical, technical and administrative. Suitable recommendations were made that should minimise risks within the business. Good risk assessment completed with a good, modified floor plan.

The student has made some excellent recommendations that meet the scenario and take into account some of the risks identified in task 1. This covers the different legislation that this would support. They have made recommendations on how these could be enforced that took into account both policies within the organisation and technical methods that could enforce it.

The student has written 2 comprehensive reports that link together but identify that they are 2 different policies. The plans take into account the identified risk of the building flooding and consider the possibility of business continuity being a big focus of the business in a world where anything could restrict access to the office/building. The student has identified both technical and people-based elements – ensuring that people know what needs doing and when.

The student has taken steps to mitigate the risks associated with both the server and the client. They have taken good steps to identify and minimise risks to both the machines in terms of security updates and anti-virus/anti-malware and also the data in terms of encryption, access controls and group policy updates.

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 is logical and a good response to the demands of the brief
	Makes use of relevant knowledge and is generally informed by the practices of the sector
	Demonstrates an understanding of some perspectives or approaches associated within the sector
	Makes good use of facts/theories/approaches/concepts
	Demonstrates breadth and depth of knowledge and understanding
	Generally selects appropriate skills/techniques/methods
	Identifies information from appropriate sources
	Makes use of appropriate information/appraises relevancy of information
	Combines information to make accurate decisions
	Makes generally sound judgements/takes appropriate action/seeks clarification and guidance
	Able to successfully tackle routine problems and make some progress on solving non-routine problems in real life situations
	Demonstrates most skills and knowledge of the relevant concepts and techniques reflected in the sector and is applied across different contexts
	Able to make some progress on unstructured problems that have not been seen before, using their knowledge to find solutions to problems
	Makes some justification for strategies for solving problems, giving explanations for their reasoning
Distinction	The evidence is logical and provides an excellent response to the demands of the brief
	Makes use of relevant knowledge and is well-informed by the practices of the sector
	Demonstrates an understanding of the different perspectives/approaches associated within the sector
	Makes excellent use of facts/theories/approaches/concepts

	Demonstrates comprehensive use of breadth and depth of knowledge and understanding
	Consistently selects appropriate skills/techniques/methods
	Identifies information from a range of suitable sources and makes use of appropriate information/ appraises relevancy of information
	Combines information to make accurate and appropriate decisions
	Makes sound judgements/takes appropriate action/seeks clarification and guidance
	Successfully tackles both routine and non-routine problems that reflect real life situations in the sector
	Effectively demonstrates skills and knowledge of the relevant concepts and techniques reflected in the sector and is applied across a variety of contexts
	Tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems
	Analyses data/information in context and applies appropriate analysis in confirming or refuting conclusions and carrying out further work to evaluate conclusions
	Justifies strategies for solving problems, giving clear 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

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	Published final version.		May 2021
v1.1	NCFE rebrand		September 2021