T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Infrastructure

Assignment 3 - Workbook - Pass

Guide standard exemplification materials

v1.1: Specimen assessment materials
January 2023
603/6901/0

Internal reference: DSS-GSEM-27

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

Digital Infrastructure

Guide standard exemplification materials

Assignment 3

Workbook - Pass

Contents

About this assignment

Introduction

All evidence should be placed in this workbook.

Save your document regularly as you work through the assignment. It is recommended you save after inserting each piece of evidence.

Submit this workbook in .pdf format at the end of the assignment using the file naming convention.

Surname_Initial_student number_Workbook3

For example Smith_J_123456789_Workbook3.pdf

Evidence

All screenshots should be numbered and linked to the task.

For example, task 1, evidence 2 would be shortened to 1.2.

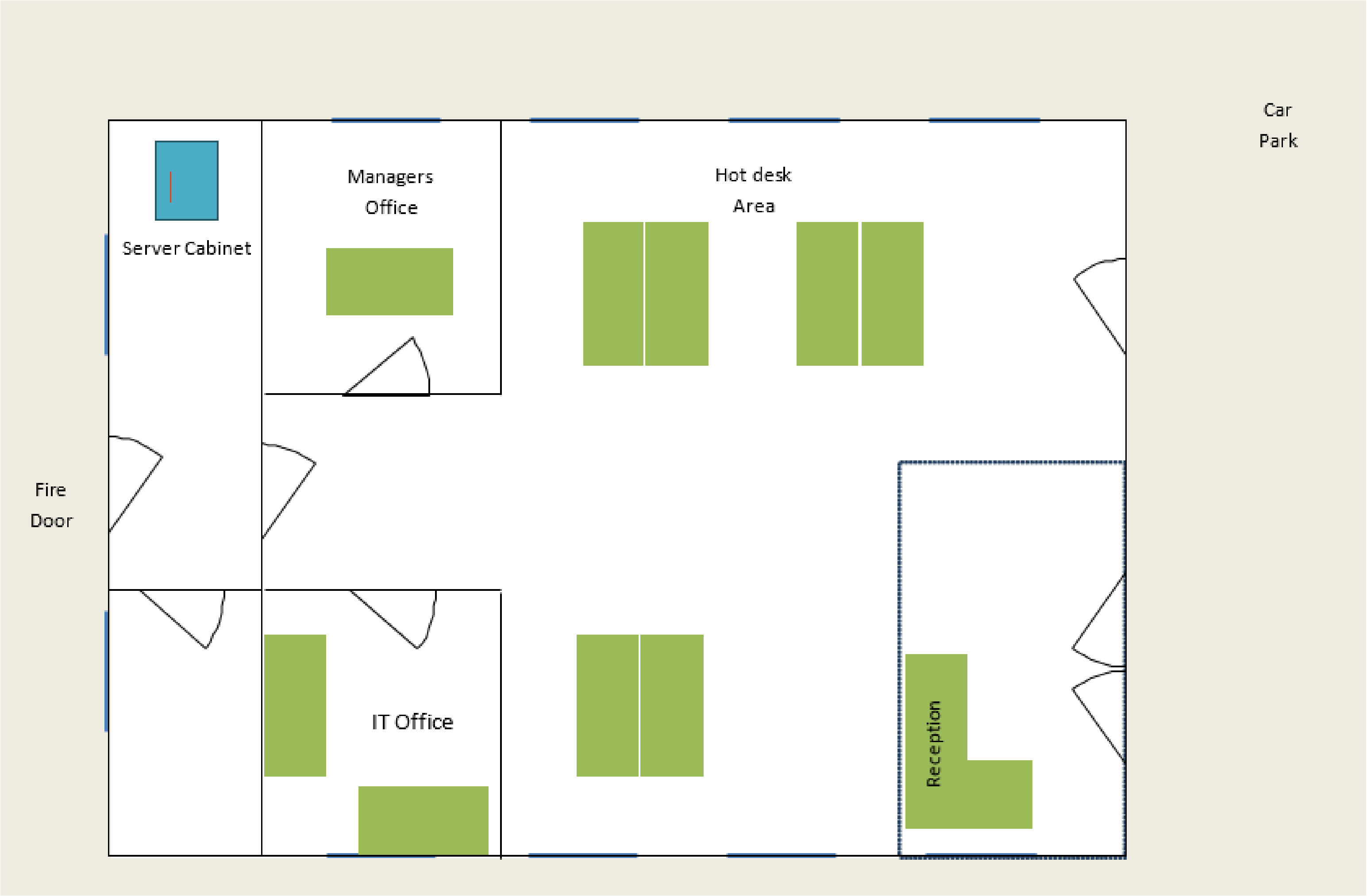
Ensure each screenshot is labelled with a brief description of what is being shown.

Task 1: risk assessment template

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

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

Task 1: York office floor plan



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 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.	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	Should someone want to access the building they would then be	They would gain access to the computers and could potentially	I would recommend the installation of a fence around the car park to minimise the access to the	Physical - preventative

				interior significantly less secure. Medium	able to do some of the other things identified within this table. Medium	access content or steal the devices. Medium	building, this would ensure that the building would become more secure.	
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	This would mean someone accessing the open plan office and not	Should someone manage to get access to the computer then they could	The installation of Kensington locks in the hot desk area would ensure that users could secure their devices whilst	Physical/administrative – deterrent

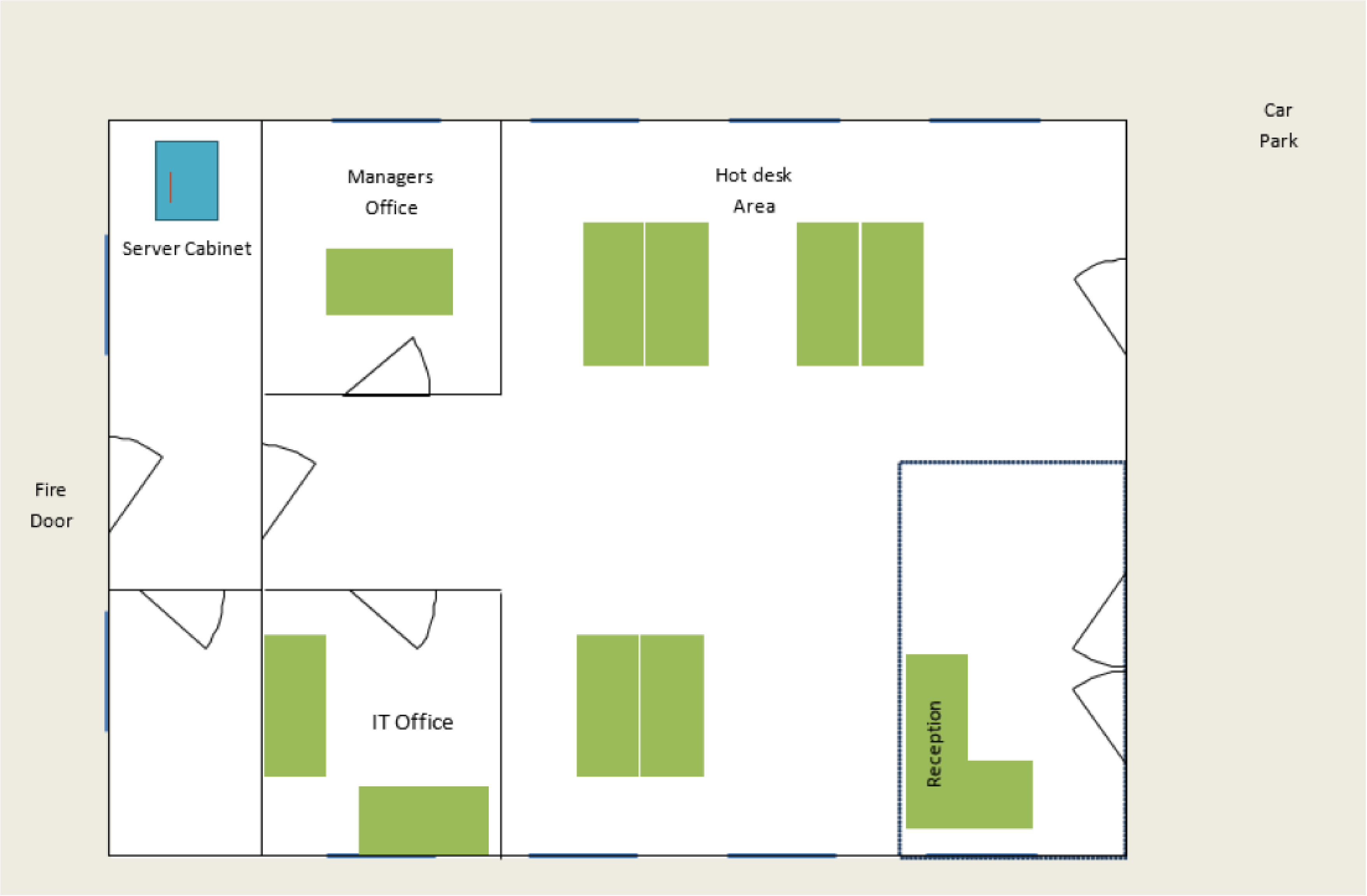
				a device or access any files left open. Medium	being noticed by anyone else, whilst possible the chances are lower. Low	either steal the device. Medium	they are in the office. The update of the company policy to ensure that these are used and signage to remind users would support this.	
7	No audit history, 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 policies 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 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	This would only become an issue should someone either misplace	The risk is potentially access to various different levels of company	The installation of Windows 10 Pro and the activation of Bitlocker would ensure that should the device be lost or	Technical – preventative.

				someone who was able to bypass the password. High	or have their laptop stolen. Medium	data dependant upon what the user had saved upon the machine. High	stolen then people would be unlikely to be able to access the data.	
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 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
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	Company Files	Potentially there could be	This would depend on	This could lead to a security	With the introduction of	Administrative /technical -

		screensaver		unauthorised access to the data if someone walked away from their computer and didn’t lock it. Medium	whether people regularly forget to lock their computers. Medium	breach of data or in extreme cases data deletion. High	policies within the company, group policies should also be altered to ensure that screens lock automatically after a set period (for example, 3 minutes).	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

Task 2

Security policy report

Password policy

There 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 GDPR (General Data Protection Regulations).

Group policy – screens should be set to go to screensaver after a set period (for example, 5 minutes) 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

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.

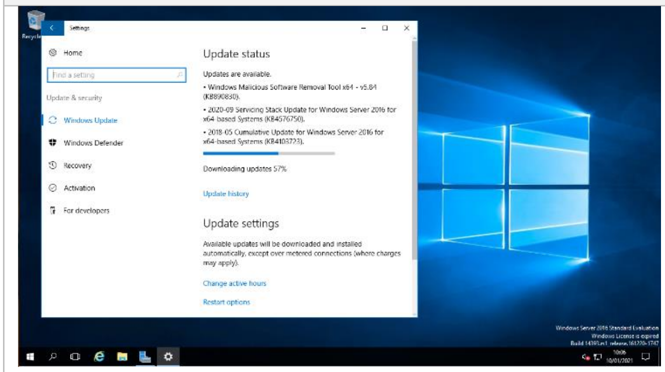
Task 4

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):



Update status

Updates are available.

- Windows Malicious Software Removal Tool x64 - v5.84 (KB890830).
- 2020-09 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB4576750).
- 2018-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4103723).

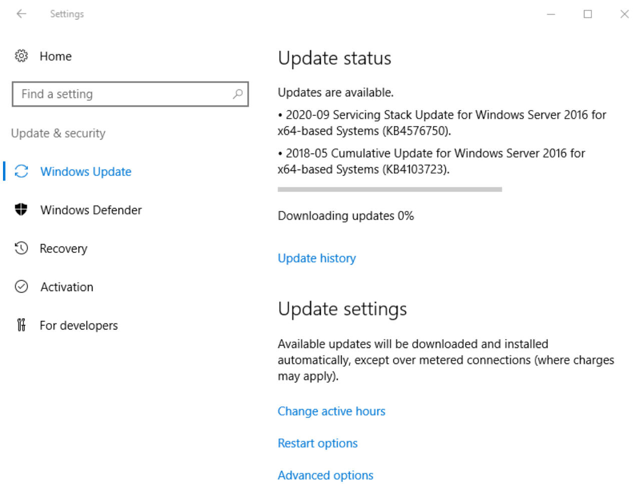
Downloading updates 57%

Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

Windows Server 2016 Standard Evaluation
Windows License is expired
Build 14393.rs1_release.161220-1747

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



Update status

Updates are available.

- 2020-09 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB4576750).
- 2018-05 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4103723).

Downloading updates 0%

Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

Any unexpected results found whilst hardening the system:
None

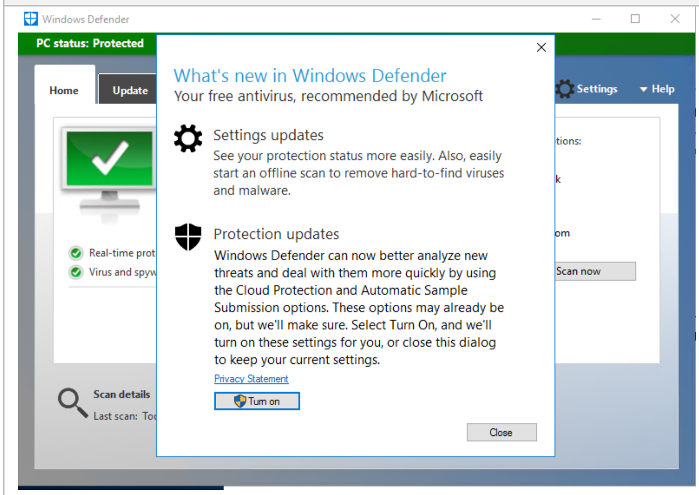
Explain how the action you have taken will better protect the system
These updates focus around security patches, and also included above is definition files for the Windows malicious software removal tool – Windows Defender.

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 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):



What's new in Windows Defender

Your free antivirus, recommended by Microsoft

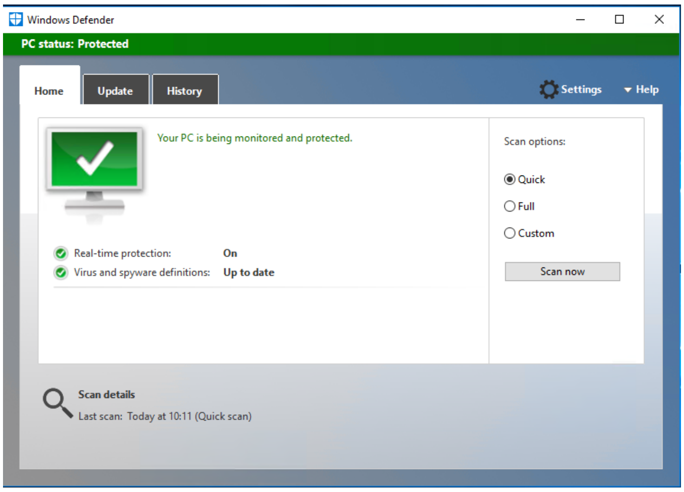
Settings updates

See your protection status more easily. Also, easily start an offline scan to remove hard-to-find viruses and malware.

Protection updates

Windows Defender can now better analyze new threats and deal with them more quickly by using the Cloud Protection and Automatic Sample Submission options. These options may already be on, but we'll make sure. Select Turn On, and we'll turn on these settings for you, or close this dialog to keep your current settings.

Privacy Statement



Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

Last scan: Today at 10:11 (Quick scan)

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

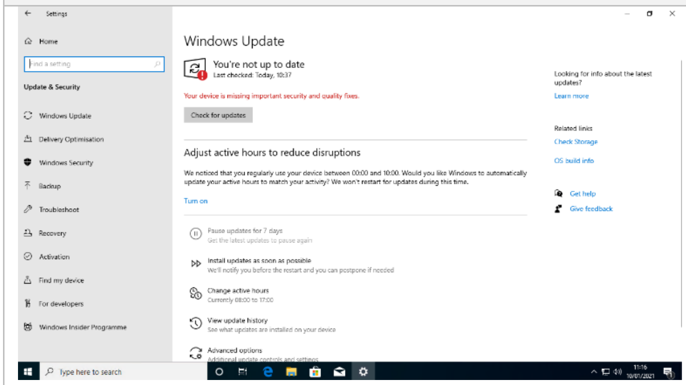
Action 3

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 Update

You're not up to date
Last checked: Today, 10:37

Your device is missing important security and quality fixes.

Check for updates

Adjust active hours to reduce disruptions

We noticed that you regularly use your device between 00:00 and 10:00. Would you like Windows to automatically update your active hours to match your activity? We won't restart for updates during this time.

Turn on

Pause updates for 7 days
Get the latest updates to pause again

Install updates as soon as possible
We'll notify you before the restart and you can postpone if needed

Change active hours
Currently 08:00 to 17:00

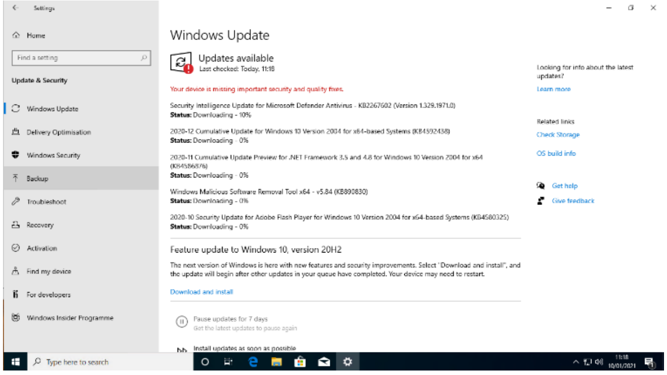
View update history
See what updates are installed on your device

Advanced options
Additional update controls and settings

Looking for info about the latest updates?
Learn more

Related links
Check Storage
OS build info

Get help
Give feedback



Windows Update

Updates available
Last checked: Today, 11:18

Your device is missing important security and quality fixes.

Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.329.1971.0)
Status: Downloading - 10%

2020-12 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB4592438)
Status: Downloading - 0%

2020-11 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Windows 10 Version 2004 for x64 (KB4586876)
Status: Downloading - 0%

Windows Malicious Software Removal Tool x64 - v5.84 (KB890830)
Status: Downloading - 0%

2020-10 Security Update for Adobe Flash Player for Windows 10 Version 2004 for x64-based Systems (KB4580325)
Status: Downloading - 0%

Feature update to Windows 10, version 20H2

The next version of Windows is here with new features and security improvements. Select 'Download and install", and the update will begin after other updates in your queue have completed. Your device may need to restart.

Download and install

Pause updates for 7 days
Get the latest updates to pause again

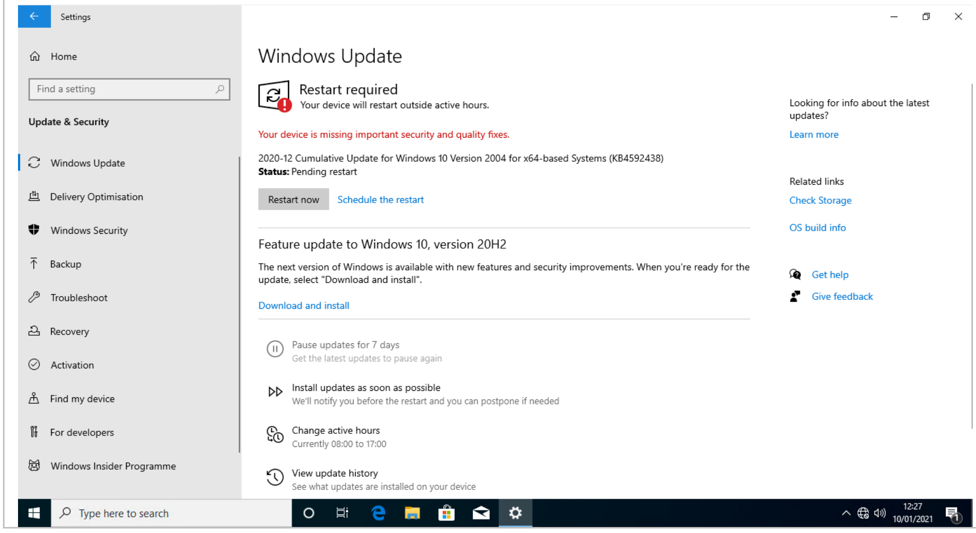
Install updates as soon as possible

Looking for info about the latest updates?
Learn more

Related links
Check Storage
OS build info

Get help
Give feedback

Windows is now installing various updates, including the Defender antivirus updates and the Windows malicious software removal tool.



Windows Update

Restart required
Your device will restart outside active hours.

Your device is missing important security and quality fixes.

2020-12 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB4592438)
Status: Pending restart

Restart now Schedule the restart

Feature update to Windows 10, version 20H2

The next version of Windows is available with new features and security improvements. When you're ready for the update, select "Download and install".

Download and install

Pause updates for 7 days
Get the latest updates to pause again

Install updates as soon as possible
We'll notify you before the restart and you can postpone if needed

Change active hours
Currently 08:00 to 17:00

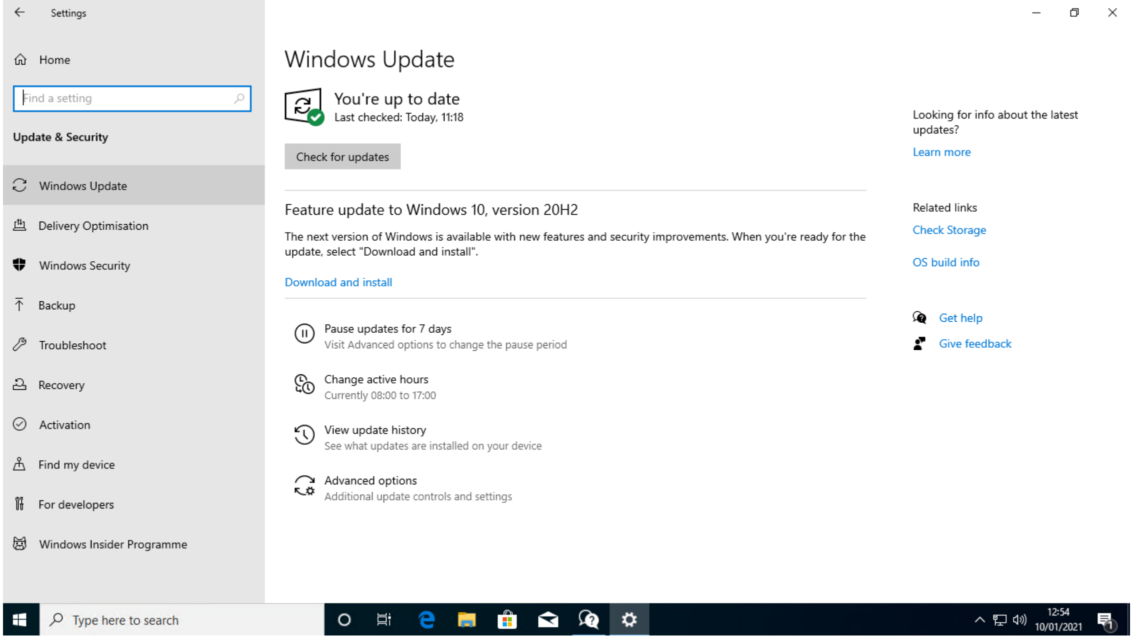
View update history
See what updates are installed on your device

Looking for info about the latest updates?
Learn more

Related links
Check Storage
OS build info

Get help
Give feedback

Fully up to date:



Windows Update

You're up to date
Last checked: Today, 11:18

Check for updates

Feature update to Windows 10, version 20H2

The next version of Windows is available with new features and security improvements. When you're ready for the update, select "Download and install".

Download and install

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 08:00 to 17:00

View update history
See what updates are installed on your device

Advanced options
Additional update controls and settings

Looking for info about the latest updates?
Learn more

Related links
Check Storage
OS build info

Get help
Give feedback

The machine was restarted as required by the updates.

Any unexpected results found whilst hardening the system:
None

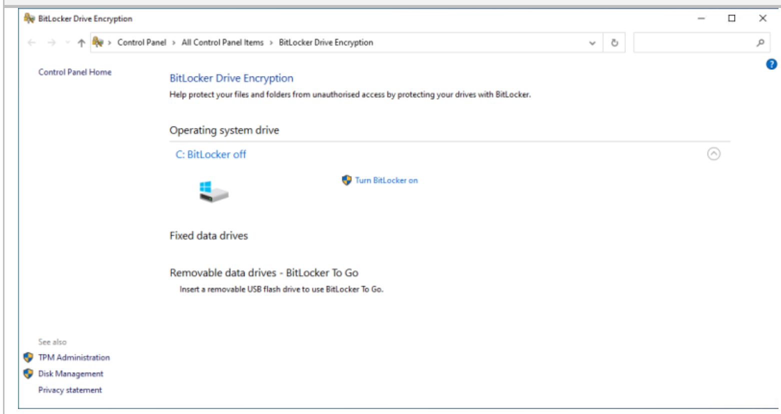
Explain how the action you have taken will better protect the system
As well as the updated security patches having the latest virus definitions will ensure that the machine has taken all precautions towards any malicious intentions.

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):


BitLocker Drive Encryption
Control Panel > All Control Panel Items > BitLocker Drive Encryption
Control Panel Home
See also
TPM Administration
Disk Management
Privacy statement

BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

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

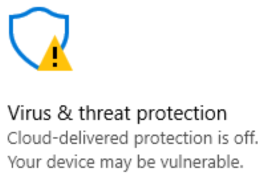
None

Action 5

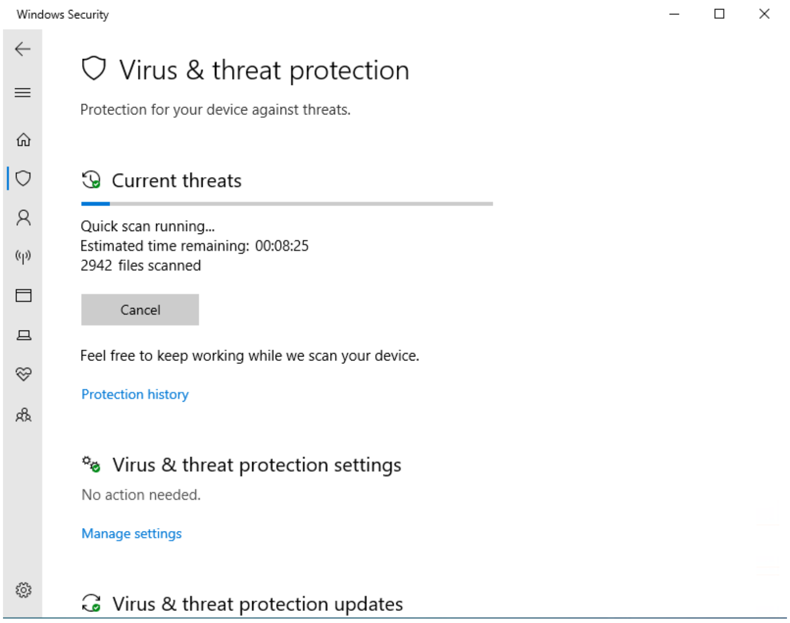
Description of action you have chosen to implement:

Windows Defender scan

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



Virus & threat protection
Cloud-delivered protection is off.
Your device may be vulnerable.



Windows Security

Virus & threat protection

Protection for your device against threats.

Current threats

Quick scan running...
Estimated time remaining: 00:08:25
2942 files scanned

Cancel

Feel free to keep working while we scan your device.

Protection history

Virus & threat protection settings

No action needed.

Manage settings

Virus & threat protection updates

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.

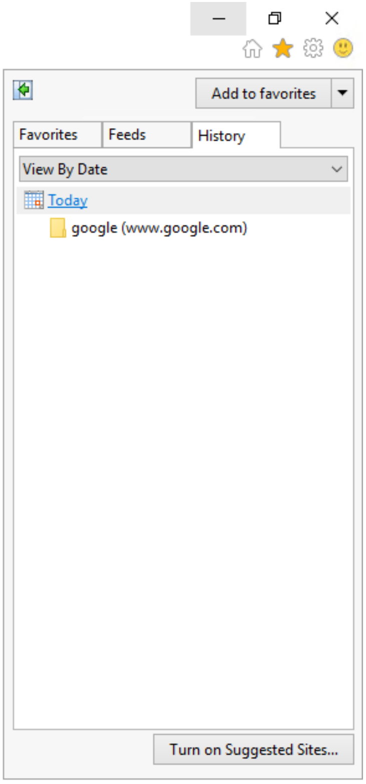
Websites accessed

None

Browser history

Please insert a screenshot of your browser history here.

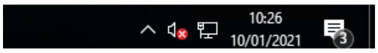
Server internet history



View By Date

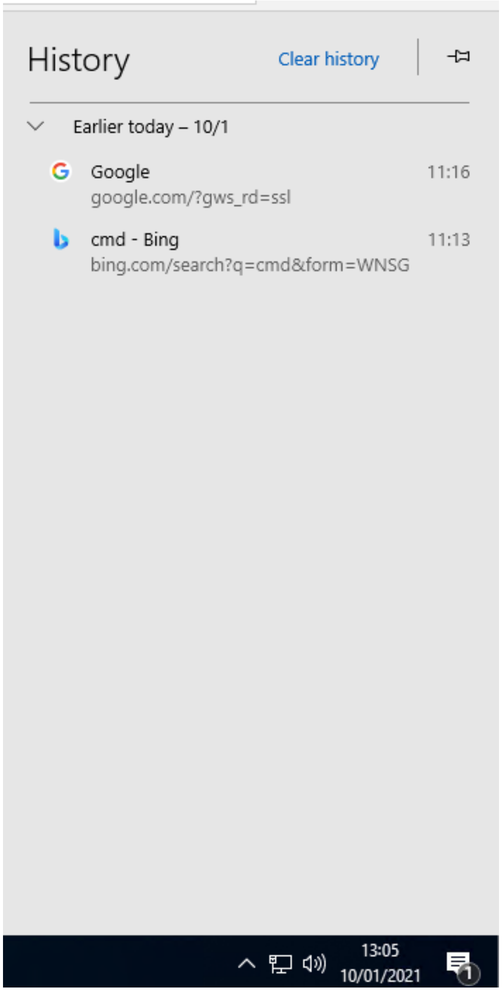
Today

google (www.google.com)



10:26
10/01/2021

Desktop internet history



History

Earlier today – 10/1

Google 11:16
google.com/?gws_rd=ssl

cmd - Bing 11:13
bing.com/search?q=cmd&form=WNSG

13:05
10/01/2021

Review and submit

You have now reached the end of the assignment. It is recommended that you review all the evidence required for the assignment to ensure all screenshots and annotations have been provided.

Save this document and convert into a .pdf for submission using the file naming convention.

Surname_Initial_student number_Workbook3

For example Smith_J_123456789_Workbook3.pdf

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.		January 2023