SITE survey. APP

SITE SURVEY REPORT

IT Audit and Health Check

Prepared for	Greystone Builders Merchants Ltd
Date	17 Sep 2026
Site	Greystone Builders Merchants, Preston
Prepared by	N. Whitfield

FORM

IT Audit and Health Check

1. Details

Project	Greystone Builders Merchants, Preston: IT audit
Customer	Greystone Builders Merchants Ltd
Site	Head office and trade counter, Preston
Site address	Riverside Trade Park, Preston PR1
Date of audit	17 Sep 2026
Auditor	N. Whitfield
What does the audit cover?	Network and internet, Servers and storage, PCs, laptops and mobiles, Cloud services and email, Backup and recovery, Accounts and security, Comms room and cabling
Number of staff who use IT	34
Number of sites	2
Who looks after IT now?	Nobody in particular
What does the customer say is not working?	Slow internet at the trade counter. Nobody is sure the backups work. Staff share one login for the stock system.
How was this checked?	Seen on site, Checked in admin consoles, Told by staff

2. Network and internet

Internet connection	Fibre to the cabinet
Download (Mbps)	68
Upload (Mbps)	16
Contracted download (Mbps)	80
Contracted upload (Mbps)	20
Download against the contract (%)	85
Upload against the contract (%)	80
Is there a second connection if the main one fails?	No

Firewall or router make and model	Router supplied by the internet provider
Does it still get security updates from the maker?	Not known
Switches	Unmanaged
Is guest Wi-Fi kept separate from the main network?	No
Is there an up to date network diagram?	No
How do staff connect from outside?	Remote desktop open to the internet

> Remote desktop open to the internet is a common way in for attackers. Recommend a VPN or a gateway with multi-factor authentication.

Photos of the cabinet and network equipment





3. Servers and cloud

Email	Microsoft 365
Where are files kept?	A mix
Are there servers or storage devices on site?	Yes

Servers and storage 1: GBM-SRV01

Name	GBM-SRV01
What it does	Stock system and shared files
Operating system and version	Windows Server 2012 R2
Does it still get security updates?	No

> Unsupported software. Cyber Essentials requires software to be licensed and supported, and removed from devices when it becomes unsupported.

Year bought	2015
Age (years)	11
Warranty or support contract	Expired
Free disk space (%)	9
Servers no longer getting updates	1
Servers with no warranty or support	1

4. PCs, laptops and mobiles

Desktops	18
Laptops	12
Company phones and tablets	8
Devices in total	38
How many run an operating system that no longer gets security updates?	5
Devices no longer getting updates (%)	13

> Unsupported software. Cyber Essentials requires software to be licensed and supported, and removed from devices when it becomes unsupported.

How are updates installed?	Automatically, nobody checks

> Updates. Cyber Essentials requires updates that fix critical or high risk vulnerabilities (a CVSS v3 base score of 7 or above) to be installed within 14 days of release.

Are laptops encrypted?	Partly
Anti-malware on every device?	Yes
Do staff use administrator accounts for day to day work?	Yes

> Cyber Essentials requires separate accounts for administrative work, with no email or web browsing from them.

Is there an up to date list of devices?	No

5. Backup and recovery

Is anything backed up?	Yes

What is backed up?	Servers, Shared files
How often?	Daily or more
Is a copy kept off site or in the cloud?	No
Is there a copy that ransomware on the network could not reach?	No
Is there a written plan for what to do if systems are lost?	No
Are servers and network equipment on a UPS?	No

6. Accounts and security

Multi-factor authentication on email and cloud services	Administrators only

> Multi-factor authentication. Cyber Essentials requires multi-factor authentication for every account on a cloud service (such as Microsoft 365), and says it should always be used for administrative accounts and any account reachable from the internet.

Are accounts closed when people leave?	Yes, eventually
Are any logins shared between people?	Yes
How are passwords looked after?	Written down or in a spreadsheet
Cyber Essentials	Never certified
Have staff had security awareness training in the last year?	No

7. Findings and recommendations

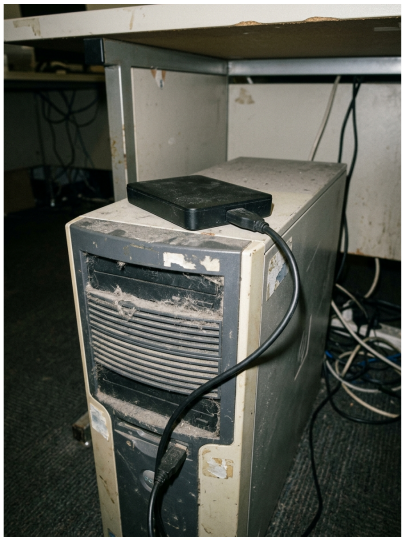
Findings 1: Accounts and security

Area	Accounts and security
Risk	High
What did you find?	Remote desktop on the stock server is open to the internet, with no multi-factor authentication.
What do you recommend?	Close it now. Give remote staff a VPN with multi-factor authentication.
Who should act on it?	C. Morley, with N. Whitfield
By when?	18 Sep 2026

Findings 2: Backup and recovery

Area	Backup and recovery
Risk	High
What did you find?	Backups go to a USB drive left plugged into the server. No off-site or offline copy, and no restore has been tested.
What do you recommend?	Add a cloud backup of the server and Microsoft 365, then test a restore.
Who should act on it?	C. Morley
By when?	15 Oct 2026

Photos or screenshots



Findings 3: Servers and storage

Area	Servers and storage
Risk	High
What did you find?	GBM-SRV01 runs Windows Server 2012 R2, which no longer gets security updates. 9% disk free.
What do you recommend?	Move shared files to SharePoint and plan a supported home for the stock system.
Who should act on it?	C. Morley
By when?	31 Dec 2026

Findings 4: Accounts and security

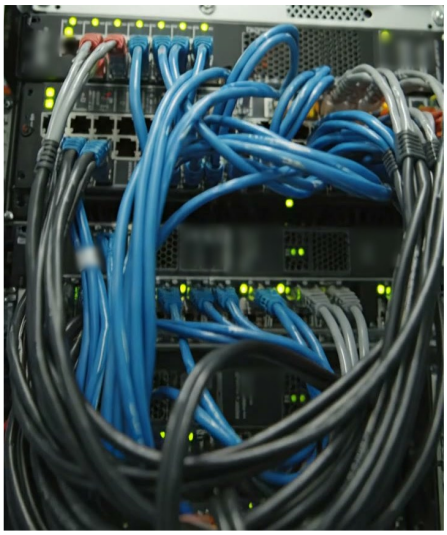
Area	Accounts and security

Risk	Medium
What did you find?	Trade counter staff share one login for the stock system, and passwords are kept in a spreadsheet on the server.
What do you recommend?	Give each person their own login and move passwords to a password manager.
Who should act on it?	C. Morley
By when?	31 Oct 2026

Findings 5: Comms room and cabling

Area	Comms room and cabling
Risk	Medium
What did you find?	Back of the rack: loose patch and power leads hang across the switch vents. Nothing labelled.
What do you recommend?	Dress and label the cabling, and fit cable management bars.
Who should act on it?	N. Whitfield
By when?	31 Oct 2026

Photos or screenshots



Findings	5
High risk findings	3
Medium risk findings	2

8. Summary and sign-off

Key controls. The form counts 14 controls from your answers: multi-factor authentication for all users, no remote desktop open to the internet, a supported firewall, no unsupported devices, updates installed and checked, encrypted laptops, anti-malware everywhere, no day to day admin accounts, an off-site and an offline backup, a tested restore, a written recovery plan, same day leavers and staff training. It is a guide for the summary, not a Cyber Essentials result.

Key controls in place (of 14)	1
Health score (%)	7
Overall	At risk: act now
Summary for the customer	The business depends on one old server that no longer gets security updates, is reachable from the internet, and has no tested backup. These need fixing first. Day to day the network works, but it is unmanaged and undocumented.
The three things to do first	1. Close remote desktop to the internet and turn on multi-factor authentication for every user. 2. Start an off-site backup and test a restore. 3. Plan the replacement of GBM-SRV01.
Anything not checked, and why	Router admin page not checked: the internet provider holds the login, so its update status is not known. The second site's PCs were counted from staff answers, not seen.
Auditor name	N. Whitfield
Auditor signature	
Customer name	C. Morley, operations director
Customer signature	