Security audit: remediation report

Client: Meridian Joinery Ltd · **Authorised by:** S. Whitcombe, Operations Director

Scope: Head office, 14 devices, plus the public-facing perimeter

Run: 4 August 2026 · **Auditor:** Alpha IT Solutions

> **Sample report.** Meridian Joinery is a fictional client. The layout, the check references and the scoring are exactly what a real Alpha IT audit produces.

Summary

Fourteen devices were checked, along with everything reachable from the internet.

Most of the basics are in place. Antivirus is running everywhere, Windows is current on twelve of fourteen machines, and the firewall is on across the estate. That is a better starting position than most firms of this size.

Three things need attention, and one of them needs it this week. Remote Desktop is open to the internet on the office server, which is how the majority of ransomware attacks on small businesses begin. The other two are ordinary housekeeping.

Overall rating: HIGH **, 47/100.** Close the Remote Desktop hole and that drops to 23.

Priority actions

#	Do this	Why it matters	Effort	Closes
1	Close Remote Desktop at the router	Anyone on the internet can reach your server's login screen	1 h	`EXT-3389`
2	Turn on BitLocker across 6 laptops	A stolen laptop is currently a data breach you must report	Half a day	`ENC-001`
3	Set a password policy	Six characters, no lockout. Guessable in minutes	30 min	`ACC-004`, `ACC-005`
4	Turn off SMBv1 on 2 machines	The protocol WannaCry used. Nothing needs it	30 min	`CFG-002`

#	Do this	Why it matters	Effort	Closes
5	Patch the two machines behind	Both missing updates rated important	1 h	`VULN-001-` HIGH

What was found

Remote Desktop is open to the internet

`EXT-3389` on the office server · **CRITICAL**

Port 3389 answers from outside your network. That is the Windows login screen, published to anyone who cares to look, and automated tools scan for it constantly.

> Confirmed from outside your network: `open tcp/3389 ms-wbt-server`

This is not theoretical. Exposed Remote Desktop is the single most common route into a small business, and the attacker does not need a clever exploit. They need one weak password, and your policy currently allows six characters.

Fix: close 3389 at the router today. If staff need remote access, put it behind a VPN so the login screen is not on the public internet. One hour, and it removes the most likely way you get attacked.

Six laptops are not encrypted

`ENC-001` across 6 devices · **HIGH**

BitLocker is off. If one of those laptops is left on a train, whoever picks it up can read every file on it by moving the drive to another machine. No password is involved.

Because you hold customer names and addresses, that is a personal data breach, reportable to the ICO within 72 hours.

Fix: enable BitLocker on each laptop and store the recovery keys somewhere central. Half a day across six machines, and it can run in the background while people work.

The password policy allows six characters

`ACC-004` and `ACC-005` · **HIGH**

Minimum length is six and there is no lockout, so an attacker can guess indefinitely without being stopped. Combined with the open Remote Desktop above, this is the pairing that gets businesses encrypted.

Fix: twelve characters minimum, or eight with a lockout after ten failed attempts. Thirty minutes, applied centrally.

SMBv1 is enabled on two machines

`CFG-002` on 2 devices · **MEDIUM**

A file-sharing protocol Microsoft retired years ago and the one WannaCry spread through in

1. Nothing on your network needs it.

Fix: remove the feature. Half an hour. Worth checking your accounts package first, as some very old line-of-business software still asks for it.

Two machines are behind on updates

`VULN-001-` HIGH on 2 devices · MEDIUM

Read directly from Windows Update, so this is fact rather than inference. Cyber Essentials requires high and critical updates applied within fourteen days.

Fix: install and reboot. An hour, out of hours.

What is already working

Nine controls verified as effective. Worth saying, because a list of only problems suggests nothing is in place.

Control	Verified
`FW-001`	Windows Firewall enabled across all 14 devices
`AV-001`	Real-time malware protection enabled everywhere
`AV-002`	Malware signatures current
`PATCH-002`	All machines on a supported Windows release
`CFG-001`	UAC enabled
`CFG-003`	Remote Desktop disabled on workstations
`CFG-007`	Secure Boot enabled
`ACC-002`	Guest accounts disabled
`RTR-001`	UPnP disabled on the router

`RTR-001` deserves a mention. UPnP lets any device on the network open holes in your firewall without asking, and it is switched on by default on most routers. Yours is off.

Cyber Essentials readiness

Control	Status
Firewalls	Action required: `EXT-3389`
Secure Configuration	Action required: `CFG-002`, `ENC-001`

Control	Status
User Access Control	Action required: `ACC-004`, `ACC-005`
Malware Protection	Meets control
Security Update Management	Action required: `VULN-001-` `HIGH`

Four of five need work before you would pass. All five are closed by the actions above, and none of them require buying anything.

This is a readiness view, not certification. The certificate is issued by an IASME-accredited body once the questionnaire is submitted.

What this audit did not cover

Host configuration was checked on Windows machines. The NAS, the two printers and the network switches were seen as devices with open ports, not audited internally.

No testing was done against third-party systems. Your accounts package is hosted by your supplier and is outside this scope.

Prepared by Alpha IT Solutions · Cyber Security & IT Support · 020 3411 1886