Restart IT

Technology review
Phase 1 findings

Gap analysis, prioritised recommendations, decisions required, initial RAID log and action plan

Client	**Example Client Ltd**
Version	**1.0, draft for discussion**
Date	**September 2026**
Prepared by	**Restart IT**

EXAMPLE REPORT

Example Client Ltd is fictional. This report shows the format and depth of a Restart IT Phase 1 review. It does not describe any real organisation.

1. Summary

Example Client Ltd is a 45-person professional services firm with one office, a Microsoft 365 Business Premium subscription, and IT supported by an external managed service provider (MSP). The firm needs Cyber Essentials to keep a major client contract that renews in early 2027. This review covered the current technology setup, the draft Cyber Essentials self-assessment, the Microsoft 365 tenant and the MSP arrangement.

Overall position

Red	**The firm would not pass Cyber Essentials today.** Three of the five control areas fail outright, and the other two have gaps to close before submitting. Most fixes are straightforward and low cost; the main constraints are device replacement lead time and getting the MSP to act promptly.

Key findings

- A legacy server is reachable from the internet over Remote Desktop (RDP). This is the most serious risk found and a common route for ransomware.
- 9 of 48 accounts have no multi-factor authentication (MFA), and older sign-in methods that bypass MFA are still allowed. Four people use a Global Administrator account for their everyday email.
- 5 laptops run Windows 10, which Microsoft stopped supporting in October 2025. None are enrolled in Extended Security Updates, so they fail Cyber Essentials automatically.
- 4 accounts belonging to people who have left are still active. One forwards all mail to a personal address outside the business.
- The MSP contract has no security responsibilities, no patching targets and no reporting. The MSP holds the only working admin credentials through a shared account.
- No one in the business owns IT risk. There is no joiners and leavers process, no current asset register and no evidence that backups have ever been test-restored.

Decisions needed from the leadership team

Six decisions are set out in section 5. Two are needed within two weeks to protect the Cyber Essentials timeline: whether to replace the Windows 10 laptops (D1), and the target date for certification (D6).

Headline plan

With the decisions made on time, the firm can close all Cyber Essentials blockers within 8 to 10 weeks and submit the self-assessment around week 12, leaving room before the contract renewal. The full plan is in section 7.

2. Scope and approach

In scope: the Microsoft 365 tenant (read-only access), device and antivirus data from Intune and Defender, the office firewall configuration (reviewed with the MSP), the draft Cyber Essentials self-assessment prepared in March 2026, and the MSP contract and service reports.

Out of scope: penetration testing, physical security, and the line-of-business application's own internal controls (the vendor was asked for evidence instead).

People consulted: Managing Director, Finance Director, Office Manager, two team leads, the MSP account manager and support engineer, and the line-of-business software vendor.

How to read the ratings

Rating	Meaning
Red	Fails a Cyber Essentials requirement or presents a high risk. Act now.
Amber	Partly in place, or a moderate risk. Plan to fix within 90 days.
Green	Meets the requirement. Keep it under review.

3. Current environment

Area	What's in place today
People and accounts	45 staff; 48 Microsoft 365 accounts (includes 4 leavers and 2 shared mailboxes with sign-in enabled)
Licensing	Microsoft 365 Business Premium, 54 licences purchased, 48 assigned
Laptops	43 Windows laptops: 38 on Windows 11, 5 on Windows 10. 31 enrolled in Intune.
Mobile phones	12 company phones (enrolled). About 10 personal phones access email through the Outlook app with no controls.
Network	One office with a managed firewall. Staff work from home 2 to 3 days a week with no VPN; cloud services are accessed directly.
Servers and storage	One on-site server running an old accounts package, reached by staff over RDP. On-site network storage (NAS) holds archived files and backs up nightly to cloud storage.
Business applications	Cloud-hosted practice management system; Microsoft 365 for email, Teams and SharePoint.
Support	MSP on an 8am to 6pm helpdesk contract. Contract renews January 2027.

4. Gap analysis

4.1 Cyber Essentials

Measured against the five Cyber Essentials technical controls. A single failing item in any area is enough to fail certification.

Control	What's required (summary)	What we found	Rating
Firewalls	Block unapproved inbound connections. No admin interface exposed to the internet without protection.	RDP (port 3389) forwarded from any internet address to the legacy server. Firewall admin page reachable from the internet with a password only.	**Red**
Secure configuration	Remove unnecessary software and accounts, change default passwords, lock devices with a PIN or biometric.	All staff have local admin rights. 12 laptops not in Intune, so their settings can't be confirmed. Personal phones accessing email are in scope but unmanaged.	**Amber**
Security update management	Only supported software. High and critical updates applied within 14 days.	5 laptops on unsupported Windows 10. Adobe Reader and Zoom more than 14 days out of date on 17 laptops. No third-party patching in place.	**Red**
User access control	Accounts only for current staff, MFA on cloud services, separate accounts for admin work.	9 accounts without MFA. 4 leaver accounts active. 4 people use Global Admin accounts for daily work.	**Red**
Malware protection	Anti-malware running and up to date on all devices.	Microsoft Defender on all Intune laptops. 2 laptops have not reported in over 30 days.	**Amber**

4.2 Microsoft 365

Area	What we found	Rating
Sign-in security	No Conditional Access policies despite Business Premium licences. Security defaults turned off. Legacy authentication allowed.	Red
Admin access	4 Global Admins, all used for daily email. MSP uses one shared admin account. No emergency (break-glass) account.	Red
Email	2 mailbox rules forward mail to personal Gmail addresses. Automatic forwarding outside the business not blocked. DMARC set to monitor only.	Amber
File sharing	SharePoint allows 'Anyone' links. 140 anonymous links active, some to client folders.	Amber
Device management	Intune in place but 12 of 43 laptops not enrolled. No compliance policies, so non-compliant devices can still reach company data.	Amber
Data protection	No backup of Microsoft 365 beyond Microsoft's standard retention. No retention policies set.	Amber
Audit logging	Unified audit log turned on and searchable.	Green
Licensing	6 unused Business Premium licences, plus 4 assigned to leavers. Savings available.	Green

4.3 Suppliers and governance

Area	What we found	Rating
MSP contract	Covers helpdesk only. No security responsibilities, patching targets or reporting. Service reports not supplied for 6 months.	Amber
Ownership of IT risk	No named owner. IT decisions are made ad hoc by whoever raises the issue.	Amber
Joiners and leavers	Informal email to the MSP. No checklist, no confirmation back. This is the cause of the active leaver accounts.	Red
Asset register	Spreadsheet last updated 2024. Doesn't match Intune.	Amber
Backup and recovery	NAS backs up nightly to cloud storage according to the MSP. No record of a test restore. No written recovery plan.	Amber
Policies	Acceptable use policy from 2019. No information security, access or device policies.	Amber

5. Prioritised recommendations

Priority 1 items remove the most serious risks and the Cyber Essentials blockers. Effort: Low is under a day, Medium is up to a week, High is more than a week or needs purchasing.

Priority 1: within 30 days

Ref	Recommendation	Owner	Effort
R1	Remove the RDP port forward. Give the few staff who need the legacy server access through a VPN with MFA, until the server is retired (D2). Restrict the firewall admin page to the office.	MSP	Low
R2	Disable the 4 leaver accounts and remove the 2 external forwarding rules, after checking with the account owners' managers.	Office Manager	Low
R3	Turn on MFA for everyone through Conditional Access, starting with a pilot group, and block legacy authentication. Confirm the practice management system works with it first (DP-02).	Restart IT with MSP	Medium
R4	Give admins separate admin accounts. Reduce Global Admins to 2 named people plus 1 emergency account. Replace the MSP's shared account with named, delegated access.	Restart IT with MSP	Medium
R5	Replace or upgrade the 5 Windows 10 laptops, subject to D1.	Finance Director	High

Priority 2: within 90 days

Ref	Recommendation	Owner	Effort
R6	Enrol the remaining 12 laptops in Intune, apply compliance policies, and remove local admin rights.	MSP	Medium
R7	Automate third-party app updates with a 14-day target and a monthly report.	MSP	Medium
R8	Limit SharePoint sharing to named people and existing guests. Review the 140 anonymous links with each team.	Restart IT	Medium
R9	Protect company data on personal phones with app protection policies, subject to D3.	Restart IT	Low
R10	Add a security schedule to the MSP contract: patching targets, monthly reporting, named access, subject to D4.	Finance Director	Medium
R11	Test-restore files from the NAS backup and write a one-page recovery plan. Decide on Microsoft 365 backup (D5).	MSP	Medium

Priority 3: after 90 days

Ref	Recommendation	Owner	Effort
R12	Submit the Cyber Essentials self-assessment once R1 to R7 are complete. Then prepare for Cyber Essentials Plus.	Restart IT	Medium
R13	Introduce a joiners and leavers checklist, a short set of IT policies, and an asset register kept in step with Intune.	Office Manager	Medium
R14	Move DMARC from monitor to quarantine, then reject, once reports show legitimate mail passing.	MSP	Low
R15	Remove unused licences at the next billing date.	Finance Director	Low

Decisions required

ID	Decision	Options	Recommendation	Owner / by
D1	Windows 10 laptops	Replace 5 laptops, or pay for Extended Security Updates for a year	Replace. Updates only delay the cost and the devices are near end of life.	Finance Director, week 2
D2	Legacy server	Move the accounts package to a cloud version, or keep the server behind a VPN	Move to cloud. Removes the server from Cyber Essentials scope.	Managing Director, week 6
D3	Personal phones	Allow with app protection, or company phones only for email	Allow with app protection. Cheaper and staff keep one phone.	Managing Director, week 4
D4	MSP arrangement	Renegotiate to add security duties, or go to market before the January renewal	Renegotiate now, and review performance in November before deciding on renewal.	Finance Director, week 4
D5	Microsoft 365 backup	Add a third-party backup service, or rely on Microsoft's retention	Add backup. Retention doesn't protect against ransomware or accidental deletion.	Finance Director, week 8
D6	Certification date	Set a target date for Cyber Essentials	Confirm the client's deadline and set the target 4 weeks before it.	Managing Director, week 2

6. Initial RAID log

Risks, assumptions, issues and dependencies as at the end of Phase 1. This log is reviewed fortnightly with the Managing Director and Finance Director during Phase 2.

Risks

ID	Risk	Rating	Owner	Mitigation	Status
R-01	Ransomware or data theft through the RDP connection exposed to the internet	**High**	MSP	R1	Open
R-02	Account takeover through accounts without MFA or through legacy sign-in	**High**	Restart IT	R3, R4	Open
R-03	Cyber Essentials not achieved before the client deadline, putting the contract at risk	**Medium**	Managing Director	D1, D6, action plan	Open
R-04	Client data exposed through anonymous links or email forwarding	**Medium**	Restart IT	R2, R8	Open
R-05	Data can't be recovered because backups have never been tested	**Medium**	MSP	R11, D5	Open
R-06	Business can't manage its own systems if the MSP relationship ends	**Medium**	Finance Director	R4, R10	Open

Assumptions

ID	Assumption	Owner	Check by
A-01	The MSP will make firewall and admin changes within its contracted hours	Finance Director	Week 1
A-02	Business Premium licences stay in place (needed for Conditional Access and Intune)	Finance Director	Ongoing
A-03	Staff are available to swap laptops during working hours	Office Manager	Week 4

Issues

ID	Issue	Rating	Owner	Action	Status
I-01	4 leaver accounts active, one forwarding mail to a personal address	**High**	Office Manager	R2	Open
I-02	2 laptops not reporting antivirus status for over 30 days	**Medium**	MSP	Locate devices, re-enrol or retire	Open
I-03	MSP service reports not supplied for 6 months	**Medium**	Finance Director	Raise at next service review	Open

Dependencies

ID	Dependency	Owner	Needed for
DP-01	Supplier lead time for replacement laptops	Finance Director	R5, Cyber Essentials submission
DP-02	Practice management vendor confirms the app works with Conditional Access	Restart IT	R3
DP-03	MSP change window for firewall work	MSP	R1

7. Action plan

A 12-week plan to reach Cyber Essentials, assuming decisions D1 and D6 are made by week 2.

When	Actions	Links to
Weeks 1 to 2	Close RDP and lock down firewall admin. Disable leaver accounts and remove forwarding. Leadership decisions on laptops and target date. Tell staff MFA is coming.	R1, R2, D1, D6
Weeks 3 to 4	MFA pilot, then all staff. Block legacy sign-in. Separate admin accounts and set up MSP named access. Order replacement laptops.	R3, R4, R5, D3, D4
Weeks 5 to 8	Enrol remaining laptops in Intune and remove local admin rights. Automated app updates. Tighten SharePoint sharing. Deploy replacement laptops.	R5 to R9
Weeks 9 to 12	Test-restore backups and write the recovery plan. Re-run the Cyber Essentials check. Submit the self-assessment.	R11, R12, D5
Ongoing	Fortnightly RAID review with leadership. Monthly MSP service review against the new security schedule.	R10, RAID log

Phase 2

In Phase 2, Restart IT leads and coordinates these actions as the firm's day-to-day internal technology team: working with the MSP and vendors to get changes made, checking and challenging supplier recommendations, keeping the RAID log current, and reporting progress to the leadership team.

Restart IT | restart-it.co.uk