# Cybersecurity Checklist for 25–50 Person Businesses (UK)

**A practical, experience-led checklist to help you reduce risk, improve governance, and avoid the common gaps we see as organisations scale.**

**Who this is for**

This checklist is designed for organisations of roughly **25–50 staff** who rely heavily on **Microsoft 365, cloud services, laptops, and remote working**, and want a clear, structured way to sense-check whether their cybersecurity is genuinely in good shape.

**Why we created this**

We see this a lot: businesses where everything looks fine on the surface. Email works, Teams works, people log in every day.

But Microsoft 365 "working" is not the same as Microsoft 365 being properly set up, enforced, and looked after.

Security drift happens quietly. Settings change over time. People join and leave. Exceptions creep in. Controls are applied manually rather than enforced by policy.

This checklist is built around what we commonly find during onboarding and security reviews, and what we put in place to make environments more secure, more consistent, and easier to govern.

**How to use it**

- Work through each section and tick what you already have in place
- Mark anything unclear as "Needs review"
- Use the **Fast Wins in 30 Days** section at the end to prioritise the most valuable improvements
- If you want to evidence progress, repeat the checklist quarterly and keep it on file

**Quick Scorecard (Executive View)**

Use this page as a fast sense-check. If you're Amber or Red in multiple areas, that's usually a sign the environment is "working" but not fully controlled.

**Score guide**

- **Green** = In place and enforced
- **Amber** = Partially in place, inconsistent, or unclear
- **Red** = Not in place / unknown / unmanaged

| Area | Green | Amber | Red |
|---|---|---|---|
| Identity & Access Control | ☐ | ☐ | ☐ |
| Microsoft 365 Secure Configuration | ☐ | ☐ | ☐ |
| Endpoint & Device Security | ☐ | ☐ | ☐ |
| Email & Phishing Protection | ☐ | ☐ | ☐ |
| Backups & Recovery | ☐ | ☐ | ☐ |
| Patch Management & Vulnerability Hygiene | ☐ | ☐ | ☐ |
| Security Awareness & Human Risk | ☐ | ☐ | ☐ |
| Governance, Policies & Evidence | ☐ | ☐ | ☐ |
| Monitoring & Detection | ☐ | ☐ | ☐ |

**If you do nothing else, prioritise these first:**

1. ☐ MFA enforced for all users and admins
2. ☐ Conditional Access in place and properly configured
3. ☐ Microsoft 365 backup in place and monitored
4. ☐ Devices centrally managed (Entra ID, Intune / MDM) and encrypted
5. ☐ Offboarding process is controlled and consistent

## Section 1: Identity & Access Control (the highest-impact area)

Identity is where most modern attacks start. Strong identity controls reduce risk dramatically, even before you add more tools.

**Checklist**

- ☐ Multi-Factor Authentication (MFA) is enforced for all users (not optional)
- ☐ MFA is enforced for all admin accounts with no exceptions
- ☐ Admin accounts are separate from day-to-day user accounts (no admin work on normal logins)
- ☐ Legacy authentication is disabled (older sign-in methods that bypass modern security)
- ☐ Password policies are appropriate and enforced centrally
- ☐ A password manager is used across the business (and actually adopted)
- ☐ Users do not share accounts or credentials
- ☐ Role-Based Access Control (RBAC) is used for admin roles
- ☐ Admin roles follow least privilege (people only have what they need)
- ☐ Access to critical systems is reviewed periodically (at least quarterly)

**What we commonly see missing (real-world)**

- MFA enabled for some users, but not enforced properly
- Admin accounts left unprotected or treated the same as normal users
- Old sign-in rules that allow access from anywhere, on any device
- Nobody can confidently answer "who owns access and security in Microsoft 365?"

**Owner:** IT provider / internal IT owner

## Section 2: Microsoft 365 Secure Configuration (the bit most firms assume is "fine")

Microsoft 365 can look completely normal and still be quietly insecure. This section focuses on secure configuration that is **enforced by policy**, not left to chance.

### Checklist

#### Identity and sign-in controls

- ☐ Conditional Access policies are in place to control access by risk and device status
- ☐ Access is restricted based on device compliance (where appropriate)
- ☐ High-risk sign-ins are detected and acted on
- ☐ Legacy authentication is disabled
- ☐ Security defaults are reviewed and enforced (not left at "whatever happened historically")

#### Admin controls

- ☐ Admin roles are tightly controlled (least privilege)
- ☐ Admin actions are auditable
- ☐ Privileged access is reviewed periodically
- ☐ Break-glass accounts exist and are secured appropriately

#### Email, SharePoint and Teams security

- ☐ External sharing is controlled and reviewed
- ☐ SharePoint and OneDrive sharing settings are not overly permissive
- ☐ Guest access is governed and reviewed
- ☐ Teams is configured with sensible external communication controls
- ☐ Mailbox rules and forwarding are controlled to reduce abuse risk

#### Logging and evidence

- ☐ Audit logging is enabled and retained
- ☐ Sign-in logs are enabled and reviewed when needed
- ☐ Alerts exist for suspicious sign-in activity and risky behaviour

### What "good" looks like

A Microsoft 365 environment where security is **enforced centrally**, aligned to recognised standards, and not dependent on individuals remembering to do the right thing.

### What we commonly see missing (real-world)

- Policies partially applied rather than enforced centrally
- Controls switched on manually but not governed
- Logging incomplete or never fully enabled

- Conditional Access either missing, outdated, or too relaxed

**Owner:** IT provider / internal IT owner

**Section 3: Endpoint & Device Security (laptops, desktops, mobiles)**

For most businesses in this size bracket, the laptop is the "office". Devices must be secure by default.

**Checklist**

- ☐ All company devices are centrally managed (Intune or equivalent)
- ☐ Full disk encryption is enforced (BitLocker / FileVault)
- ☐ Firewall is enabled on all devices
- ☐ Automatic updates are enabled and monitored
- ☐ Anti-malware / EDR is deployed and monitored
- ☐ Local admin rights are restricted (users are not local admins)
- ☐ Screen lock is enforced with an inactivity timeout
- ☐ USB and removable storage use is controlled where appropriate
- ☐ Lost/stolen device response exists (remote wipe capability)
- ☐ Mobile phones used for email are managed (or access is restricted)

**What we commonly see missing (real-world)**

- Devices not properly enrolled into management
- Encryption not enforced consistently
- Users with admin rights "because it's easier"
- No clear view of what devices exist, who owns them, or whether they're compliant

**Owner:** IT provider / internal IT owner

**Section 4: Email & Phishing Protection (where most incidents begin)**

Email remains the most common entry point for cyber incidents. You don't need perfection, but you do need the basics properly handled.

**Checklist**

- ☐ Phishing and malicious link protection is enabled
- ☐ Spam filtering is properly configured and monitored
- ☐ External sender warnings are enabled
- ☐ Users cannot auto-forward company email to personal addresses
- ☐ SPF, DKIM and DMARC are configured
- ☐ Suspicious attachments are blocked or sandboxed
- ☐ Reporting phishing is simple for staff (one click where possible)
- ☐ Shared mailboxes are governed (not a free-for-all)
- ☐ Departed users' mailboxes are handled securely

**What we commonly see missing (real-world)**

- Email is "working" but controls are loose
- Forwarding and mailbox rules are uncontrolled
- No one is monitoring patterns or repeated phishing attempts

**Owner:** IT provider / internal IT owner

**Section 5: Backups & Recovery (this is what saves you when something goes wrong)**

Backups are not about convenience. They're about survival.
And Microsoft 365 data should not be assumed to be backed up in the way most businesses expect.

**Checklist**

- ☐ Critical data is identified (what you cannot lose)
- ☐ Microsoft 365 is backed up separately (email, OneDrive, SharePoint)
- ☐ Backups run at least daily for critical systems
- ☐ Backup success is monitored (failures are caught and fixed quickly)
- ☐ Backups are protected from ransomware (separate access, immutability/offline copy where possible)
- ☐ Recovery is tested (even lightly, at least quarterly)
- ☐ You know who is responsible for recovery and how long it will take
- ☐ Retention is appropriate (not too short, not uncontrolled forever)

**What we commonly see missing (real-world)**

- "We assumed Microsoft backs everything up"
- Backups exist but nobody checks whether they're actually working
- Recovery has never been tested
- Backup access is not separated, meaning ransomware can potentially encrypt the backups too

**Owner:** IT provider / internal IT owner

### Section 6: Patch Management & Vulnerability Hygiene

Most successful attacks rely on known weaknesses. Patch management is one of the highest ROI security habits you can build.

**Checklist**

- ☐ Operating system updates are enforced and monitored
- ☐ Third-party applications are patched (not just Windows/macOS)
- ☐ Unsupported devices are removed or replaced
- ☐ Vulnerability scanning is performed periodically (even lightweight)
- ☐ Critical vulnerabilities are prioritised and resolved quickly
- ☐ There is a clear process for exceptions (and exceptions are documented)

**What we commonly see missing (real-world)**

- Updates left to individuals
- Old machines kept “because they still work”
- No visibility of vulnerable software versions across the business

**Owner:** IT provider / internal IT owner

**Section 7: Security Awareness & Human Risk (simple, but essential)**

Most organisations don't need staff to become cybersecurity experts. They need them to spot the obvious risks and act quickly.

**Checklist**

- ☐ Security awareness training is provided at least annually
- ☐ Phishing simulations are run occasionally (even quarterly is good)
- ☐ Staff know how to report suspicious emails and incidents
- ☐ A simple "what to do if you clicked" process exists
- ☐ New starters receive basic security onboarding
- ☐ Staff understand safe password habits and MFA
- ☐ Staff understand the risk of sharing data via personal apps/accounts

**What we commonly see missing (real-world)**

- No training, or training that's treated as a checkbox
- People unsure what counts as an incident
- "I didn't report it because I wasn't sure"

**Owner:** Leadership + IT provider

**Section 8: Governance, Policies & Evidence (what good looks like when someone asks)**

This is the part that helps you respond confidently to:

- client due diligence questionnaires
- cyber insurance questions
- regulatory expectations
- board-level scrutiny

**Checklist**

- ☐ You have an acceptable use policy
- ☐ You have a BYOD policy (if personal devices are used)
- ☐ You have a backup policy and retention expectations
- ☐ You have a leavers/offboarding process
- ☐ You have a simple incident response plan (even one page)
- ☐ You have a clear owner for IT risk decisions internally
- ☐ Exceptions are documented (not just "informal knowledge")
- ☐ You can evidence what is enforced (not just what is intended)

**What we commonly see missing (real-world)**

- Policies exist but aren't aligned to what's actually happening
- No evidence trail when asked "how do you know this is enforced?"
- Responsibility unclear (IT provider assumes client owns it, client assumes IT provider owns it)

**Owner:** Leadership + IT provider

**Section 9: Monitoring & Detection (catching problems early)**

The goal is not to "monitor everything". The goal is to detect meaningful issues early and respond properly.

**Checklist**

- ☐ Endpoint protection is deployed and monitored (EDR)
- ☐ Suspicious sign-ins are detected and reviewed
- ☐ Alerts are configured for risky behaviour (where possible)
- ☐ Logs exist and can be used during an investigation
- ☐ You know what happens if there is an incident (who does what, and how fast)
- ☐ You have a sensible escalation process for urgent issues

**What we commonly see missing (real-world)**

- Tools exist, but nobody is actively watching or responding
- Alerts go to an inbox nobody monitors
- Unclear response steps when something genuinely suspicious happens

**Owner:** IT provider / internal IT owner

## Fast Wins in 30 Days (high impact, realistic, and measurable)

If you want the biggest improvements with the least wasted effort, these are the moves that typically matter most for a 25–50 person business.

**Week 1: Lock down identity properly**

1. ☐ Enforce MFA for all users and all admins
2. ☐ Remove admin rights from day-to-day accounts
3. ☐ Disable legacy authentication
4. ☐ Confirm who owns Microsoft 365 security internally and externally

**Week 2: Get Conditional Access and device control right**

5. ☐ Implement Conditional Access policies that reflect your actual risk profile
6. ☐ Ensure devices are centrally managed and compliant (Intune/MDM)
7. ☐ Enforce disk encryption and screen lock policies

**Week 3: Make backups and recovery real**

8. ☐ Implement a Microsoft 365 backup (if not already in place)
9. ☐ Start monitoring backup success and fix failures quickly
10. ☐ Run a basic recovery test and document the result

**Week 4: Reduce the human risk**

11. ☐ Roll out a short security awareness refresher
12. ☐ Make phishing reporting simple and visible
13. ☐ Publish a one-page "what to do if you clicked" guide

**If you complete these, you'll usually be in a dramatically stronger position within 30 days.**

### Certification Readiness (and how to demonstrate maturity)

This checklist is designed to help you strengthen your cybersecurity posture in a way that is structured, enforceable, and defensible.

It also supports preparation for:

- **Cyber Essentials**
- **Cyber Essentials Plus**
- **Alignment to recognised frameworks such as CIS**

Even if you are not pursuing formal certification immediately, working through these controls helps you demonstrate that:

- security is being managed intentionally
- key risks are being reduced
- controls are enforced and evidenced
- governance exists beyond “IT is working”

**Closing Note**

If you'd like a second opinion, or you want to confirm whether your Microsoft 365 environment is properly set up, enforced, and actively looked after, this is the sort of review we complete during onboarding and ongoing managed service delivery.