INNOVA SECURE

Protect What Matters.

PRACTICAL GUIDE

Cyber Security Essentials Checklist

An honest, plain-English checklist for small and medium-sized businesses — covering the controls that stop most breaches.

Five Controls · **Backup & People** · **Built on Microsoft**

InnovaSecure — A division of Innova Group

v1.0 · July 2026

innovasecure.tech

BEFORE YOU START

Most breaches exploit basic gaps, not clever ones.

This checklist exists because the security industry tends to talk about sophisticated threats, while the incidents that actually harm smaller businesses are almost always mundane.

A reused password. An account without multi-factor authentication. A laptop three months behind on updates. A shared folder still accessible to someone who left last year. None of these require a determined attacker — they simply require nobody to have checked. Spending on advanced tooling while these basics go unaddressed is like fitting an alarm to a house with the front door open.

So this is a checklist of fundamentals. It is organised around the five controls of **Cyber Essentials**, the UK government-backed scheme, because that framework is a sensible, well-tested account of what "the basics" actually means. Where a control connects to tools you likely already own in Microsoft 365, we have said which — because for most businesses the capability is already paid for and simply switched off.

How to work through it. Go control by control and answer honestly. A box you cannot confidently tick is not a failure; it is useful information. Some items will be quick to fix in an afternoon, others will need planning. The aim is an accurate picture of where you stand, not a full sheet of ticks.

You do not need to be technical to use this. If an item is unclear, or you are not sure who in your business owns it, that ambiguity is itself worth noting — unclear ownership is one of the most common reasons basic controls quietly lapse.

> A NOTE ON HONESTY
>
> This checklist is not a sales tool, and there is no score that requires you to buy anything. If you work through it and find you are in good shape, that is a genuinely good outcome. If you find gaps, most are fixable with configuration rather than expenditure.

INNOVA SECURE

THE FRAMEWORK

The Five Controls

Get these five right and you close the gaps behind the overwhelming majority of incidents affecting businesses of your size.

The five controls below are the structure of this checklist, and of Cyber Essentials itself. They are deliberately unglamorous. Each one addresses a specific, well-understood route by which businesses are compromised — and each is achievable without specialist infrastructure.

01 Firewalls & Internet Gateways

Controlling what can reach your network and devices from the internet, and making sure nothing is exposed that does not need to be.

02 Secure Configuration

Removing default settings, unused accounts and unnecessary software — the things that ship switched on and are rarely revisited.

03 User Access Control

Making sure people have the access they need and no more, with strong authentication on every account. This is where Microsoft 365 does most of the work.

04 Malware Protection

Ensuring every device has active, current protection, and that staff cannot easily run something they should not.

05 Security Update Management

Keeping operating systems, applications and firmware patched within a sensible window — the single most effective control on this list.

CONTROL ONE

Firewalls & Internet Gateways

The boundary between your business and the internet. The goal is simple: nothing is reachable from outside unless it genuinely needs to be.

- [ ] **Every internet connection sits behind a firewall**
  Office broadband, and any site or remote location. The router supplied by your provider usually includes one — the question is whether it is configured or simply present.
- [ ] **Default administrator passwords have been changed**
  Routers and firewalls ship with well-known credentials that are published online. This is one of the most exploited weaknesses there is, and one of the quickest to fix.
- [ ] **Remote administration from the internet is disabled**
  Unless there is a documented reason and it is protected by strong authentication, the management interface should not be reachable from outside your network.
- [ ] **No unnecessary ports or services are open**
  Inbound rules accumulate over years — often for a supplier or system long since retired. Each one should be justifiable today, not merely historical.
- [ ] **Laptops used outside the office have their own firewall enabled**
  A device on hotel or home Wi-Fi has no office firewall protecting it. The host firewall built into Windows and macOS should be on and enforced centrally.
- [ ] **Firewall rules are reviewed at least annually**
  With someone named as responsible. A rule set nobody has read in three years is a rule set nobody understands.

WHERE MICROSOFT HELPS

Windows Firewall can be configured and enforced across every device centrally through **Microsoft Intune**, so protection travels with the laptop rather than depending on the network it happens to be on. **Availability depends on your Microsoft 365 licence.**

CONTROL TWO

Secure Configuration

Devices and services arrive configured for convenience, not for security. This control is about closing what you were never using in the first place.

- [ ] **Unused accounts are removed or disabled**
  Former staff, contractors, old test accounts and shared logins nobody can attribute. Dormant accounts are attractive precisely because no one notices activity on them.
- [ ] **Software and apps you do not use have been removed**
  Every application is a potential way in and something else to patch. If nobody can say who uses it, it probably should not be there.
- [ ] **Devices require a password, PIN or biometric to unlock**
  Enforced by policy rather than left to each person, and applied to phones and tablets used for work email as well as laptops.
- [ ] **Screens lock automatically after a period of inactivity**
  Fifteen minutes or less is a reasonable standard, and it matters most in shared offices, client sites and public spaces.
- [ ] **Hard drives are encrypted**
  BitLocker on Windows, FileVault on macOS. Without it, a stolen laptop is a data breach; with it, it is an insurance claim.
- [ ] **Auto-run and auto-play of removable media is disabled**
  So plugging in an unknown USB stick does not execute anything on its own.
- [ ] **You know what devices and services you actually have**
  A current list of laptops, phones, servers and cloud services in use. You cannot secure or patch what nobody has written down, and this is the item most often missing.
- [ ] **New devices follow a documented standard build**
  Rather than each machine being set up by hand, differently, by whoever happens to be free that day.

> WHERE MICROSOFT HELPS
>
> **Intune** configuration profiles let you define one standard — encryption, lock timeouts, PIN requirements, permitted software — and apply it to every device automatically, including new starters' laptops on first sign-in. **Availability depends on your Microsoft 365 licence.**

CONTROL THREE

User Access Control

Identity is the real perimeter. If you can only improve one area immediately, multi-factor authentication usually delivers the biggest reduction in risk.

- [ ] **Multi-factor authentication is enabled on every account**
  Every user, without exception, including senior staff and anyone who has asked to be excluded. MFA prevents the vast majority of attacks that rely on stolen passwords, though it is not effective against every technique.
- [ ] **Administrator accounts are separate from day-to-day accounts**
  Nobody should read email and browse the web from an account that can reconfigure your tenancy. Admin rights are used deliberately, not held permanently.
- [ ] **Users have only the access their role requires**
  Access tends to accumulate as people change roles and never has anything removed. Permissions should reflect the job someone does now.
- [ ] **Leavers are removed the same day they leave**
  Accounts, email, file access and third-party services — a documented process, not a memory exercise.
- [ ] **No shared or generic logins**
  If several people use one account, you cannot tell who did what — and you cannot revoke one person's access without disrupting everyone.
- [ ] **Access is reviewed regularly**
  At least twice a year, with an owner. This is where quiet privilege creep gets caught.
- [ ] **Sign-in is restricted by conditions where sensible**
  For example, blocking sign-in from countries you do not operate in, or requiring a managed device for access to sensitive data.
- [ ] **Aspirational: phishing-resistant MFA for key accounts**
  Passkeys or FIDO2 security keys cannot be intercepted the way codes and prompts can. Worth considering for administrators and finance staff once the basics are in place.

WHERE MICROSOFT HELPS

Entra ID and **Conditional Access** cover most of this control, and MFA and access reviews are configuration rather than new purchases. Note that Conditional Access and the more advanced identity protection features are not in every plan. **Availability depends on your Microsoft 365 licence.**

CONTROL FOUR

Malware Protection

Not a question of whether you have antivirus, but whether it is active everywhere, current, and actually being watched by someone.

- [ ] **Every device has active malware protection**
  Including laptops used from home and any machine that only connects occasionally. Coverage gaps are usually the devices nobody thinks of as "on the network".
- [ ] **Protection updates automatically**
  Daily at minimum. Protection that is a fortnight out of date is protection against a fortnight-old threat landscape.
- [ ] **Someone actually sees the alerts**
  A detection nobody reads is not protection. There should be a named person or partner who reviews alerts and knows what to do with them.
- [ ] **Email is filtered for phishing and malicious attachments**
  Email remains the most common delivery route by a wide margin, so this is where filtering earns its keep.
- [ ] **Malicious links are checked when clicked, not just when sent**
  Attackers often weaponise a link after the email has passed the initial scan, so time-of-click protection matters.
- [ ] **Web and DNS filtering blocks known-bad destinations**
  Stopping a device reaching a malicious site or command-and-control server catches things that slip past email filtering, and is inexpensive to add.
- [ ] **Logs are kept long enough to investigate**
  Sign-in and audit logs are often retained for only 30 days on lower licence tiers. If you needed to establish what happened last quarter, could you?
- [ ] **Staff cannot install software freely**
  Standard users should not hold local administrator rights. This single change prevents a great deal of malware from ever executing.

WHERE MICROSOFT HELPS

Microsoft Defender covers this control end to end — endpoint protection on every device, email filtering, and time-of-click link checking — with one console showing what has been detected across the business. **Availability depends on your Microsoft 365 licence.**

CONTROL FIVE

Security Update Management

The least interesting control and one of the most effective. A great many successful attacks exploit a vulnerability for which a fix was already available — though phishing and stolen credentials remain at least as common a starting point.

- [ ] **Operating systems update automatically**
  Windows and macOS, on every device — not deferred indefinitely by users who dismiss the prompt each morning.
- [ ] **Applications are patched too, not just the OS**
  Browsers, Office, PDF readers and line-of-business software. Application vulnerabilities are exploited at least as often as operating-system ones.
- [ ] **Critical patches are applied within 14 days**
  This is the Cyber Essentials standard and a sound benchmark regardless of whether you seek certification.
- [ ] **Nothing in use has passed end of support**
  Unsupported operating systems and software receive no fixes at all, so no amount of diligence elsewhere compensates.
- [ ] **Router, firewall and network device firmware is updated**
  The most commonly forgotten item on this page, and one of the most exposed.
- [ ] **Phones and tablets used for work are kept current**
  If it reaches company email or files, it is in scope — including personal devices used for work.
- [ ] **You can see patch status across all devices**
  Reporting matters: without it, "we think everything is up to date" is an assumption rather than a fact.

WHERE MICROSOFT HELPS

Intune enforces update policies and reports compliance per device, so you can demonstrate that patching is happening within your chosen window rather than hoping that it is. **Availability depends on your Microsoft 365 licence.**

RESILIENCE

Backup & Business Continuity

Not one of the five controls, but the one that decides whether a bad day becomes an existential one. The question is never whether you will need to recover something — only whether you can.

- [ ] **Business-critical data is backed up automatically**
  Including data in Microsoft 365. Cloud services provide resilience against their own failures, not against your staff deleting things or ransomware encrypting them.
- [ ] **At least one backup copy is isolated from your network**
  Ransomware deliberately seeks out and encrypts reachable backups. A copy it cannot touch is the copy that saves you.
- [ ] **You have actually tested a restore**
  Recently, and end to end. An untested backup is a hypothesis, and failed restores are discovered at the worst possible moment.
- [ ] **You know how much data loss you could tolerate**
  An hour? A day? Your backup frequency should follow that answer rather than a default someone set years ago.
- [ ] **You know how long recovery would take**
  And whether the business can function for that long. This is the number worth knowing before you need it.
- [ ] **There is a written plan for a serious incident**
  Who is called, who decides, who speaks to customers, and what is done first. It need not be long — it needs to exist and be findable when systems are down.

> WORTH KNOWING
>
> Microsoft 365 retains deleted items for a limited period by default, which is often mistaken for a backup. For most businesses it is not sufficient on its own, and a dedicated backup of 365 data is a sensible addition.

THE HUMAN LAYER

Your People

Staff are described as the weakest link so often that it has become unhelpful. Given the right conditions they are your most effective line of defence — the people most likely to notice something is wrong.

What makes the difference is not an annual training video. It is a culture where reporting something odd is quick, welcomed and never punished, so that a mistake surfaces in minutes rather than being quietly hidden for a fortnight.

- [ ] **Staff know how to report something suspicious**
  One obvious route, and a response that thanks them. If reporting feels like inviting blame, people stop doing it.
- [ ] **People can recognise a phishing attempt**
  Including the convincing ones that reference real colleagues, live invoices and current projects rather than obvious scams.
- [ ] **There is a verification step for payment changes**
  A phone call to a known number before any bank details are changed. Invoice fraud costs UK businesses more than most technical attacks.
- [ ] **Nobody is expected to bypass security to do their job**
  If a control makes work impossible, people route around it. Friction that has no explanation is friction that gets ignored.
- [ ] **Password practice is supported, not just mandated**
  A password manager — Bitwarden, 1Password or similar — together with MFA achieves far more than forced monthly rotation, which mostly produces predictable variations.
- [ ] **New starters are briefed in their first week**
  Before habits form, and as part of onboarding rather than an afterthought.
- [ ] **AI tools have clear ground rules**
  Which tools are approved and what company or client data may go into them. Microsoft Copilot within your tenancy is a very different proposition to a public chatbot.

MAKING SENSE OF IT

Where You Stand

Count the boxes you could not confidently tick. That number is more useful than any score, because it tells you where to start.

0 – 3 gaps

A strong position. Close the remaining items, then move from doing the basics to being able to evidence them — which is where certification becomes straightforward.

4 – 10 gaps

Typical for a business without dedicated IT, and mostly fixable through configuration. Prioritise MFA, patching and backup, in that order.

11 or more

Meaningful exposure, though rarely as expensive to resolve as it appears. This usually reflects an environment that grew without a plan rather than neglect.

Unsure

If you could not answer many items either way, the first task is visibility. You cannot manage what you cannot see, and an assessment resolves that quickly.

IF YOU FIX ONLY THREE THINGS

- [ ] **Turn on multi-factor authentication everywhere**

  Usually the highest-value change available, and often achievable in days. Check what your current Microsoft 365 licence includes before assuming extra cost.

- [ ] **Get patching under control and visible**

  Automatic updates on every device, applications included, with reporting that shows it is genuinely happening.

- [ ] **Test that you can actually restore**

  Pick something important and recover it. You will either gain real confidence or discover a serious problem while it is still cheap to fix.

ON CERTIFICATION

If most boxes are ticked, **Cyber Essentials** is likely within reach and increasingly expected by larger customers and public-sector buyers. Treat it as evidence of being secure rather than the reason for it. We help businesses prepare for and achieve certification; the certificate itself is issued by an IASME-licensed Certification Body.

INNOVA
GROUP

NEXT STEPS

Gaps are normal. Leaving them isn't.

If working through this raised questions, or you would like an honest second opinion on where you stand, we are happy to talk. A security assessment gives you a clear picture without obligation, and most of what it finds is fixable through configuration rather than expenditure.

If you are already in good shape, we will tell you that too — and leave you to get on with your work.

INNOVASECURE

Security assessments & reviews
Cyber Essentials support
innovasecure.tech

THE GROUP

Innova Technologies Group Ltd
Hull, United Kingdom
innovagroup.tech
hello@innovagroup.tech

ALSO IN THIS SERIES

Cloud Migration Readiness Template
Process & Automation Opportunity Finder
IT Health Check
Choosing a Technology Partner

FOUR DISCIPLINES, ONE PARTNER

- **InnovaSystems** — Secure. Stable. Supported.
- **InnovaWorks** — Building What's Next.
- **InnovaCloud** — Cloud Without Complexity.
- **InnovaSecure** — Protect What Matters.

Technology That Works. Innovation That Lasts.