CYBER ESSENTIALS READINESS CHECKLIST

2026

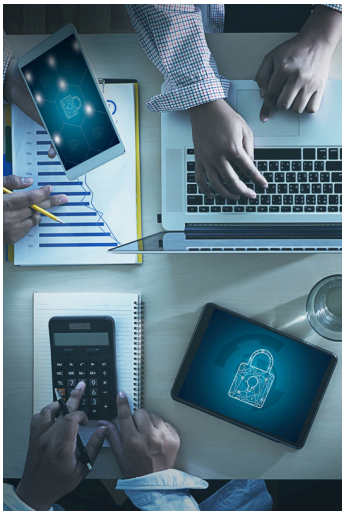
Your five-control self-assessment for UK businesses

Aligned with IASME, NCSC and UK Government guidance

WHY THIS CHECKLIST EXISTS

Over half of UK businesses suffered a cyber attack or breach in the last twelve months the highest figure on record. The uncomfortable truth is that the majority of those incidents could have been prevented with five technical controls that take days, not months, to implement.

That framework is Cyber Essentials. It is backed by the UK Government, administered by IASME, and increasingly required by public-sector contracts and cyber insurance providers. More importantly, it works: organisations that implement the five controls properly significantly reduce their exposure to ransomware, phishing, credential theft and unauthorised access. This checklist gives you an honest view of where your business stands today, before you apply, before you renew, or simply before the next attempted breach lands in your inbox.



Use this document as

- A pre-application self-assessment before you start your Cyber Essentials submission.
- An internal audit tool to check that your existing controls are still in place.
- A briefing document to share with your IT team or managed service provider.
- Evidence of due diligence for clients, insurers or board reviews.

Who it's for

Business owners, operations directors and IT managers in UK SMEs, particularly those handling client data, working with public-sector contracts, or operating under regulatory frameworks such as ISO 27001, GDPR or sector-specific compliance.

Prefer to skip the self-assessment?
If you'd prefer an experienced engineer to walk through your environment with you, we offer a no-obligation Cyber Essentials Readiness Review. We'll identify the gaps, quantify the risk, and provide you with a clear remediation plan usually within 5 working days.

- Book your readiness review at systemforce.co.uk

1. FIREWALLS AND INTERNET GATEWAYS

Firewalls are your first line of defence between the internet and everything inside your business.

Misconfigured or out-of-date firewalls remain one of the most common entry points for attackers targeting UK SMEs usually because someone left a default password in place, or opened a port "temporarily" three years ago and never closed it.

Self-assessment

- A firewall is deployed at every internet entry point including remote sites and home workers.
- Default administrator passwords have been changed on all firewall and network devices.
- Only essential ports and services are exposed to the internet.
- Remote administration is restricted to VPN or other secure access methods never open to the public internet.
- Firewall firmware is updated on a documented schedule.
- Inbound rules are reviewed at least annually and removed when no longer needed.

What good looks like

A well-configured firewall has no unnecessary open ports, does not expose RDP or admin interfaces directly to the internet, and uses modern remote access methods such as VPN or Zero Trust Network Access.

Configuration changes are logged, reviewed and reversible.

SFIT insight: We routinely encounter firewalls that were correctly configured at install but have drifted over the years due to ad-hoc changes. An annual firewall audit catches this drift before an attacker does.

2. SECURE CONFIGURATION

Out of the box, most devices and applications are configured for convenience rather than security.

Secure configuration means hardening systems before they go into production, removing what isn't needed, and applying the principle of "least functionality" if it isn't required, it isn't installed.

Self-assessment

- All devices are deployed from a standardised, hardened build not configured ad-hoc.
- Default configurations have been reviewed and tightened across all systems.
- Unused software, services and user accounts are removed.
- Auto-run is disabled for removable media.
- Screen lock is enforced at no more than 10–15 minutes of inactivity.
- Administrative interfaces are not publicly accessible.
- New devices are not connected to the production network until they are hardened.

What good looks like

Devices roll out from a known-good image with security baselines pre-applied. There is a documented build standard.

Anyone in your team could pick up a new laptop and tell you what should and shouldn't be on it.

SFIT insight: Many breaches we investigate trace back to a single device that was deployed in a hurry a temporary contractor's laptop, a meeting-room PC, an old workstation "just for now". Standardised builds eliminate this entire category of risk.

3. USER ACCESS CONTROL

User access control ensures that only the right people can access the right systems and data and that when someone leaves, their access rights are revoked. According to Microsoft, multi-factor authentication alone blocks more than 99% of account compromise attacks. There is no other control with that level of return on effort.

Self-assessment

- Every user has a unique account no shared logins, anywhere.
- The principle of least privilege is applied users only access what their role requires.
- Administrators have separate accounts for admin tasks and day-to-day work.
- Multi-Factor Authentication is enforced on Microsoft 365, VPN and all administrative accounts.
- Leaver accounts are disabled within 24 hours of departure ideally on the same day.
- Access rights are reviewed at least quarterly, or whenever a role changes.
- Privileged accounts are monitored, and their activity is logged.

What good looks like

Admin rights are tightly controlled, and the list of who has them fits on a single page. MFA is enforced everywhere it can be not just "available". Joiners, movers and leavers follow a documented process so nothing is missed.

SFIT insight: The most common gap we see is leaver accounts left active for weeks or months usually because nobody owns the offboarding process. Define the owner, automate the trigger, and this risk effectively disappears.

Not sure where you stand on MFA?
Most Microsoft 365 tenants we audit have MFA partially enabled but not fully enforced leaving exploitable gaps. We can run a free Microsoft 365 security check and tell you exactly which accounts are exposed.

- Request your Microsoft 365 security check at systemforce.co.uk

4. MALWARE PROTECTION

Malware protection defends your business against viruses, ransomware, info-stealers and the steady stream of phishing-delivered payloads landing in inboxes every day.

Cyber Essentials sets a baseline; in 2026, the realistic expectation is Endpoint Detection and Response (EDR) backed by active monitoring not standalone antivirus.

Self-assessment

- Endpoint protection is deployed on every device workstations, laptops, servers and mobile devices where applicable.
- Real-time protection is enabled and cannot be disabled by end users.
- Definitions and engine updates are automatic and verified.
- Email filtering is in place anti-phishing, anti-spam, attachment scanning and link rewriting.
- Web filtering blocks access to known malicious and high-risk sites.
- Staff have received recent (within 12 months) phishing awareness training.
- Phishing simulations are run on a regular cycle, with results tracked over time.

What good looks like

EDR is in place across the estate and is monitored either internally or by a SOC. Email and web filtering catch the majority of threats before they reach a user.

When a phishing email does land, your staff are confident enough to recognise it and report it through a defined channel and they actually do.

SFIT insight: Phishing remains the number one initial attack vector for UK businesses. Technology stops most of it, but the small percentage that gets through is where well-trained staff make all the difference. Treat awareness training as an ongoing programme, not a tick-box exercise.

5. SECURITY UPDATE MANAGEMENT

Unpatched systems are the most reliably exploited vulnerability in cyber attacks because they are the easiest to find and weaponise.

Cyber Essentials requires critical and high-severity updates to be applied within 14 days of release. In practice, the businesses that take this seriously patch faster, and the ones that don't get caught out.

Self-assessment

- Critical and high-severity security updates are applied within 14 days of release across all in-scope devices.
- Operating system updates are automated wherever possible.
- Third-party applications (browsers, PDF readers, productivity tools, line-of-business apps) are kept up to date.
- Unsupported software and operating systems are either removed or upgraded no end-of-life systems on the network.
- Vulnerability scanning is performed on a regular schedule, and findings are remediated.
- There is a documented emergency patching process for critical vulnerabilities (e.g. zero-days).

What good looks like

Patching is centralised, monitored and reported. You can answer the question "which devices are missing the latest critical update?" in minutes, not days.

End-of-life software has been identified and either replaced or formally risk-accepted never just ignored.

SFIT insight: When ransomware lands, the first thing the attacker checks is what's unpatched. Closing the patching gap is one of the highest-impact security investments a business can make and one of the easiest for an outsourced team to deliver consistently.

BEYOND CYBER ESSENTIALS: SUPPORTING CONTROLS

Cyber Essentials is a baseline, not a finishing line. The following controls are not required for certification, but they are what separate a business that has "passed" from one that is genuinely resilient.

- Backups are tested regularly not just configured. Untested backups have a habit of failing exactly when you need them.
- Systems and infrastructure are monitored, ideally 24/7, with alerts that someone actually responds to.
- An incident response plan is documented, communicated, and rehearsed at least annually.
- All staff receive ongoing security awareness training, not just at induction.
- Vulnerability scanning and remediation are run on a defined cycle, with results reviewed by management.
- Sensitive data is identified, classified and protected appropriately particularly under GDPR and ISO 27001.

COMMON CYBER ESSENTIALS FAILURES

These are the issues that most often cause UK businesses to fail their Cyber Essentials assessment. If any of them apply to you, address them before you submit.

- Multi-Factor Authentication is not enforced on Microsoft 365 accounts.
- Remote Desktop Protocol (RDP) ports are exposed directly to the internet.
- Shared user accounts exist ("reception", "warehouse", "admin").
- End-of-life operating systems or applications remain in production use.
- Backups are configured but have never been tested by restoring from them.
- Default administrator passwords on routers, firewalls or printers have not been changed.
- Leaver accounts remain active for weeks after the person has left.
- There is no documented patching process patches happen "when someone gets round to it".

If three or more of these apply to your business, you are not ready to certify and more importantly, you are exposed to threats that the Cyber Essentials controls are specifically designed to prevent.

Your final readiness check

Before you apply for Cyber Essentials, confirm that:

- All five control areas are fully implemented across every in-scope device and user.
- You have evidence available, screenshots, policies, configuration exports, to support each answer.
- Staff are aware of relevant security policies and what's expected of them.
- Your systems are aligned with current IASME requirements (these change check the latest version).
- Someone in the business owns the certification and the ongoing maintenance of the controls.

HOW SYSTEM FORCE IT CAN HELP

Achieving Cyber Essentials is not just about passing an assessment. It is about building the foundations that protect your business, your clients and your reputation every day, not just on audit day.

System Force IT delivers:

- Cyber Essentials and Cyber Essentials Plus readiness assessments.
- Remediation and implementation support we don't just tell you the gaps, we close them.
- Ongoing managed security services aligned to NCSC and IASME guidance.
- 24/7 monitoring, patching and compliance management.
- ISO 27001 alignment for businesses ready to take the next step.

Ready to find out where you stand?
Book a Cyber Essentials Readiness Review with System Force IT. One of our security engineers will assess your current posture against all five controls, identify gaps, and provide a clear plan to certify and stay certified.

- Book your free readiness review at systemforce.co.uk

Or call us directly: 01452 701355 We're based in Gloucestershire and work with businesses across the UK.

Authoritative sources and further reading

- IASME Cyber Essentials: iasme.co.uk/cyber-essentials
- NCSC Small Business Guide: ncsc.gov.uk/collection/small-business-guide
- NCSC Cyber Essentials Overview: ncsc.gov.uk/cyberessentials/overview
- UK Cyber Security Breaches Survey: gov.uk/government/statistics/cyber-security-breaches-survey
- Microsoft Security Best Practices: learn.microsoft.com/en-us/security

This document is provided for general guidance only and does not constitute formal certification advice. IASME sets Cyber Essentials requirements, which may change; always refer to the current version before applying.

System Force I.T.
Secure IT Simplified

Want a free Cyber Essentials readiness review with System Force IT?

We run free, no-obligation reviews for UK SMEs.
Written report in 7 working days.
No sales pitch, no follow-up unless you ask for one.

Book at systemforce.co.uk
Or call us directly: 01452 701355

System Force IT | supporting UK businesses since 2006.

UKAS ISO/IEC 27001: 2022 Certified | Microsoft Solutions Partner | Certified 3CX Partner | Cyber Essentials Practitioners | RIPE NCC Member

Next Step:

Book your free Cyber Essentials readiness review.

01452701355

www.systemforce.co.uk

sales@systemforce.co.uk