Cyber Essentials cheat sheet

Cyber Essentials is the UK government-backed baseline for cyber security. You answer a questionnaire about how your business is set up, and an accredited body checks it. Pass, and you get a certificate that lasts a year.

It matters because customers ask for it, some public sector contracts require it, and it stops the most common attacks. It is not a technical exam. It is five basic habits done properly.

THE 5 CONTROLS AT A GLANCE

1	2	3	4	5
Firewalls	**Secure settings**	**Updates**	**User access**	**Malware protection**
Keep the bad traffic out.	No defaults, nothing spare.	Patch the serious stuff fast.	Right people, right rights, MFA on.	Stop nasty software running.

★ **Star = bang for buck.** These fix the most risk for the least effort, and most often cause a failed assessment.

Keep the door shut, and the house tidy

1 Firewalls

What it is: A gatekeeper between your devices and systems and the internet. It decides what traffic gets in.

WHAT GOOD LOOKS LIKE

- A firewall protects your network or cloud servers, and it blocks incoming connections by default.
- Only the ports you genuinely need are open, and someone knows why each is open.
- Laptops have their own firewall switched on, so they stay protected on home, hotel and café Wi-Fi.
- The default password on any router or firewall has been changed.

BIGGEST WINS

- ★ **Never expose admin screens to the internet.** Cloud consoles, databases and management pages should be reachable only through a VPN, an allow-list or MFA, not open to the world.
- ★ **Turn on the built-in firewall on every laptop.** It is free, takes seconds and is checked on the questionnaire.

WHERE PEOPLE TRIP UP

- A rule opened "just for testing" that never got closed.
- Home routers still using the password printed on the sticker.

2 Secure configuration

What it is: Setting things up safely instead of leaving the factory settings.

WHAT GOOD LOOKS LIKE

- Default passwords are changed and every account has its own strong password.
- Software and accounts you do not use are removed or switched off.
- Devices lock after a short period of inactivity and need a PIN, password or biometric to unlock.
- Auto-run is off, so a USB stick cannot start something on its own.
- Passwords are long (a few random words works), unique, and kept in a password manager.

BIGGEST WINS

- ★ **Delete what you do not use.** Old accounts, trial software and unused apps are free attack surface.
- ★ **Use a password manager.** It makes unique, long passwords realistic for everyone, which is the single biggest habit change.

WHERE PEOPLE TRIP UP

- Leftover accounts from former staff, suppliers or old projects.
- A "temporary" shared login that became permanent.

Patch fast, and limit who can do what

3 Security update management

What it is: Installing fixes for known weaknesses before someone uses them against you.

WHAT GOOD LOOKS LIKE

- Everything runs software the maker still supports. Anything past end of life is replaced or removed.
- Automatic updates are on for operating systems, browsers and apps.
- Critical and high-severity fixes are installed within **14 days** of release.
- Someone owns this and checks it on a regular rhythm, even if it is only a short weekly slot.

BIGGEST WINS

- ★ **Retire unsupported software.** An old operating system that no longer gets fixes is the most common reason people fail.
- ★ **Learn the 14-day rule.** It is simple, measurable and exactly what an assessor looks for.
- Turn on automatic updates and let the machine do most of the work.

WHERE PEOPLE TRIP UP

Phones and tablets that nobody remembers to update.

Updates downloaded but waiting for a restart that never happens.

Code libraries and plug-ins used in your own software, which count too.

4 User access control

What it is: Making sure only the right people can get in, and only to what they need.

WHAT GOOD LOOKS LIKE

- Everyone has their own account. No shared logins.
- Admin rights are given only when needed, and admins use a separate account for admin work, not for email and web browsing.
- **Multi-factor authentication (MFA) is on for every cloud service that offers it**, and always for admin accounts.
- When someone leaves, their access is removed straight away.
- Accounts are reviewed now and then so nobody keeps access they no longer need.

BIGGEST WINS

- ★ **Switch on MFA everywhere.** Email, cloud, code, finance, password manager. It blocks most account takeovers and is one of the cheapest fixes there is.
- ★ **Separate admin from everyday use.** If your daily account is also an administrator, one bad click gives an attacker everything. This catches out many small teams.
- ★ **Have a same-day leaver routine.** A short checklist is enough.

WHERE PEOPLE TRIP UP

Admin rights on the account used for email.

MFA turned on for most services but missed on one or two, often the code repository or the domain registrar.

Switching on MFA personally but never requiring it for the whole organisation account.

Stop the nasties, then check yourself

5 Malware protection

What it is: Stopping malicious software from running on your devices.

WHAT GOOD LOOKS LIKE

- Every computer has anti-malware running, kept up to date, with real-time scanning on.
- Phones and tablets install apps only from the official app store.
- Risky content is limited: suspicious downloads and macros are blocked or controlled.
- The protection is built-in or managed, so it does not depend on anyone remembering.

BIGGEST WINS

★ **Use what is already built in.** Microsoft Defender on Windows and the protection in macOS and mobile app stores meet the need for most small businesses. No extra spend required.

- Keep it switched on and updating. A tool that is installed but off does nothing.

WHERE PEOPLE TRIP UP

- Protection turned off to fix a slow machine and never turned back on.
- Servers and personal devices assumed to be "someone else's problem".

The 8 most common ways people fail

1. Software that is no longer supported by its maker.
2. Critical fixes older than 14 days.
3. MFA missing on one or more cloud services.
4. Daily account is also an admin account.
5. Default passwords left on routers or devices.
6. Old accounts for leavers or suppliers still active.
7. Admin pages or databases open to the internet.
8. Unclear scope: devices or cloud services that were forgotten.

Check these tasks off to get ahead

- [ ] MFA on every cloud service
- [ ] Admin account separate from daily account
- [ ] Automatic updates on, nothing unsupported
- [ ] Critical fixes installed within 14 days
- [ ] Firewall on, no admin pages open to the internet
- [ ] Default passwords changed, unused accounts removed
- [ ] Anti-malware on and updating
- [ ] Leaver checklist exists and is used

Cyber Essentials is the foundation. ISO 27001 is the whole building.

Cyber Essentials proves your basics are sound. It is deliberately narrow: it looks at your technology set-up and says little about how you manage risk, people, suppliers or incidents. That is where larger customers, banks and regulated firms often want more, and where ISO 27001 comes in.

WHAT CYBER ESSENTIALS DOES NOT COVER

- A risk assessment: knowing which threats matter most to *your* business.
- Written policies that everyone has read and agreed.
- How you choose and check suppliers who handle your data.
- What you do when something goes wrong: plans, roles, deadlines.
- Backups you have actually tested, and a recovery plan.
- Staff awareness and training.
- Regular review and improvement, so security does not decay.

HOW YOUR CYBER ESSENTIALS WORK CARRIES ACROSS

Cyber Essentials control	Where it lands in ISO 27001 (Annex A, 2022)
Firewalls	A.8.20 Networks security, A.8.22 Segregation of networks
Secure configuration	A.8.9 Configuration management
Security updates	A.8.8 Management of technical vulnerabilities
User access control	A.5.15 Access control, A.5.18 Access rights, A.8.2 Privileged access rights, A.8.5 Secure authentication
Malware protection	A.8.7 Protection against malware

KEY TAKEAWAY

Everything you did for Cyber Essentials counts. It is roughly a head start on one part of ISO 27001.

Get started with Gapless, free, today.

Gapless is self-serve ISO 27001 software. It builds your risk register, Statement of Applicability and policies, and keeps your evidence in one place. You still choose your own certification body for the audit.

getgapless.com