The Cyber Essentials Readiness Workbook

Score your business against all five controls — before you pay for certification.

Hemanth Vishnu Akula

ISO 27001:2022 Lead Auditor · vCISO · Founder & CEO, Authex Labs

Version 1.1 · Checked against the Cyber Essentials “Willow” question set (v3.2)

hemanthvishnuakula.com/resources

How to use this workbook

This workbook is for the owner, operations lead, or "the person IT stuff lands on" at a small or medium business. No security background is assumed.

Set aside **60–90 minutes**. Work through it in order:

1. **Part 1** defines what's actually in scope — most failed first attempts go wrong here, not at the technical controls.
2. **Part 2** walks the five controls. Each has a plain-English explanation, the most common ways SMBs fail it, and a self-assessment checklist. Answer honestly: **Yes**, **Partial**, or **No**. You're diagnosing, not decorating.
3. **Part 3** turns your answers into a score, a traffic-light readiness band, and a prioritised remediation plan.

By the end you will know three things: **where you stand, what to fix first, and how long certification realistically takes from your position.**

One rule while you fill it in: *if you're not sure, the answer is No.* Certification assessors verify; so should you.

Why enterprises keep asking for this

If you're reading this, an enterprise customer, a tender document, or an insurer has probably already asked whether you hold Cyber Essentials. That's not bureaucracy — it's how UK supply chains now manage risk.

What Cyber Essentials is. A UK government-backed certification (run by the NCSC with IASME as the delivery partner) that verifies your business has five baseline technical controls in place. It is deliberately not a heavyweight standard: it covers the controls that stop the *commodity* attacks responsible for the large majority of SMB breaches — not targeted espionage, but the automated scanning, phishing payloads, and credential stuffing that hit every business, every day.

The two levels:

	Cyber Essentials	Cyber Essentials Plus
How it's assessed	Verified self-assessment — you answer the official question set; a board member signs a declaration; an assessor reviews	Everything in CE, **plus** an independent technical audit of a sample of your systems
Typical effort (SMB)	Days to a few weeks of preparation	CE first, then the audit — within three months of your CE certification
Who asks for it	Most enterprise procurement, insurers	MoD and defence supply chain, some public-sector contracts, security-mature enterprise buyers

Why it's worth the effort, in order of hard value:

1. **Contracts.** Cyber Essentials is mandatory for many UK government contracts (and the MoD requires CE Plus in much of its supply chain). Increasingly, enterprise procurement teams use it as a binary filter: no certificate, no vendor onboarding.
2. **The 80/20 of actual security.** The five controls genuinely block the attacks most likely to hit you. This isn't compliance theatre — patching, MFA, and removing default passwords is where real-world breaches die.
3. **Insurance.** Certification can unlock included cyber insurance for smaller organisations and smooths underwriting questions for everyone else.
4. **Sales velocity.** A current certificate turns a three-week security questionnaire exchange into a one-line answer.

What it costs. Certification fees are tiered by organisation size and change periodically — check the current fee on the IASME website rather than trusting any PDF (including this one). The real cost is preparation time, which is exactly what Parts 1–3 of this workbook let you estimate.

Validity. Certificates last 12 months. The controls are meant to be *lived*, not crammed annually — the scoring sheet in Part 3 works as a quarterly self-check too.

Part 1 — Scope: the part nobody warns you about

Assessors don't fail SMBs on exotic technology. They fail them on **scope**: the laptop nobody mentioned, the home worker on an ancient Windows machine, the cloud app that "doesn't count" (it counts).

1.1 What's automatically in scope

Work through this list and tick what applies to your business. Everything ticked is inside your assessment boundary:

- ☐ **Every laptop, desktop, and server** your business uses — owned or leased
- ☐ **Every phone and tablet** that accesses business data or services (email counts)
- ☐ **BYOD — personally owned devices** used for work. A director answering email on a personal iPhone puts that iPhone in scope. (Narrow exception: devices used *only* for voice calls, text messages, or as a multi-factor authenticator are out.)
- ☐ **Home workers' devices** — anyone working from home regularly. Their home *router* is not in scope (you don't control it), which is exactly why their device's own software firewall must be on (Control 1).
- ☐ **All cloud services** holding business data or providing business functions — Microsoft 365 or Google Workspace, accounting software, CRM, file storage, your website's hosting, code repositories. Cloud is **always in scope**; the question is only who is responsible for each control (you, the provider, or both).
- ☐ **Internet-facing infrastructure** — routers, firewalls, VPS instances, anything with a public IP your business controls.

1.2 Whole organisation or a sub-set?

You can certify the whole organisation or a defined sub-set (e.g. "UK operations only" or a network-segregated business unit).

Default to whole-organisation. It's what buyers expect — a certificate that excludes half your business invites exactly the questions you got certified to avoid. Sub-set scope is legitimate mainly when a genuinely segregated legacy environment can't yet meet the controls, and you have a dated plan to fix or retire it.

> **Instant-blocker check:** software or operating systems that no longer receive security updates (Windows 10 after end of support, old Android phones, that Server 2012 box) are an **automatic fail** if they're in scope. Your options: upgrade, remove, or properly segregate them out of scope before you apply. "We hardly use it" is not a control.

1.3 Asset inventory — devices

Fill this in now; it becomes your evidence pack later. Add rows as needed.

#	Device (make/model)	Who uses it	OS + version	Still supported by vendor?	Owned / BYOD	Notes
1				Y / N		
2				Y / N		
3				Y / N		
4				Y / N		
5				Y / N		
6				Y / N		
7				Y / N		
8				Y / N		

Any "N" in the supported column is a red flag for the whole assessment. Deal with those rows first.

1.4 Asset inventory — cloud services

#	Service	What it holds / does	Who administers it	MFA available?	MFA enforced?
1				Y / N	Y / N
2				Y / N	Y / N
3				Y / N	Y / N
4				Y / N	Y / N
5				Y / N	Y / N
6				Y / N	Y / N

A "Y / N" mismatch in the last two columns (available but not enforced) is one of the most common — and fastest to fix — failures in the whole scheme.

1.5 Network boundaries

One or two sentences each — plain English is fine:

- Where does your network meet the internet? (office router, cloud-only, co-working space…)
- Any port forwarding / services published to the internet? What and why?
- How do remote workers connect to business systems? (directly to cloud apps, VPN…)

Part 2 — The five controls

Each control: what it demands and why → how SMBs actually fail it → your checklist → evidence to collect → quick wins.

Scoring, used throughout: **Yes = 2 · Partial = 1 · No = 0.** "Partial" means true for some devices/users but not all — and in this scheme, *not all* usually means *not passing*, so treat every Partial as a to-do.

Control 1 — Firewalls

What it demands. Every in-scope device sits behind a correctly configured firewall — the boundary firewall in your router for office networks, and the device's own software firewall everywhere (which is what protects home and mobile workers, since their home routers are outside your control). Inbound connections are blocked unless there's a documented reason. Nobody can reach your router's admin page from the internet without strong protection.

Why. Automated scanners probe every public IP on the internet, continuously. An exposed admin interface or a forgotten open port is how "we're too small to be a target" businesses get breached — the scanner doesn't know your size.

The five most common SMB failures:

1. The office router still has its default admin password (printed on the sticker).
2. Software firewalls assumed on, never checked — especially on Macs, where it ships **off**.
3. Port forwarding set up years ago for a CCTV system or NAS, never reviewed, still open.
4. Router admin interface reachable from the internet "because the IT guy works remotely".
5. Home workers counted as "outside the network" and ignored entirely.

Checklist 1 — Firewalls

#	Item	Yes (2)	Partial (1)	No (0)
1.1	Every laptop, desktop, and server has its software firewall turned ON (Windows Defender Firewall, macOS firewall)			
1.2	The admin password on your internet router / boundary firewall has been changed from the default			
1.3	Inbound connections are blocked by default; nothing is exposed to the internet without a documented business need			
1.4	You can list every internet-exposed service (port forwards, published apps) — and each one is still needed			
1.5	The router/firewall admin interface is NOT reachable from the internet — or where it must be, it's protected by a second factor or an IP allow-list, with the need documented			
1.6	Home/remote workers' devices have their software firewall enabled (their home routers are not your control)			
1.7	UPnP is disabled on the boundary router, or every rule it created is known and justified			
1.8	Firewall rules are removed when no longer needed (someone owns this)			
1.9	Guest Wi-Fi is separated from the business network			
1.10	Cloud servers (VPS, hosted boxes) have host firewalls / security groups set to default-deny inbound			
	Control 1 total (/20)			

Evidence to collect now: screenshot of router admin password change / settings page; screenshots of firewall status on a sample of devices; your port-forwarding list with one-line justifications.

Quick wins (this week, free): turn on the macOS firewall fleet-wide; change the router admin password; delete every port forward you can't explain; switch off UPnP.

Control 2 — Secure configuration

What it demands. Devices and services run with deliberate settings, not factory defaults: default passwords changed, unused software and accounts removed, autorun disabled, and every device protected by authentication — with brute-force protection (a PIN of at least 6 digits, a password, or biometrics, plus lockout or throttling after repeated wrong guesses).

Why. Default credentials and forgotten software are the attacker's favourite furniture. Every app you don't use is attack surface you're maintaining for free.

The five most common SMB failures:

1. Devices set up ad-hoc by whoever was free that day — no standard build, no checklist.
2. Pre-installed bloatware and trial software never removed.
3. Shared tablets/till devices with no PIN, "for convenience".
4. Old user accounts on machines (and in cloud apps) from people who left in 2023.
5. Cloud services running on out-of-the-box settings — public sharing defaults, legacy protocols enabled.

Checklist 2 — Secure configuration

#	Item	Yes (2)	Partial (1)	No (0)
2.1	Default passwords have been changed on every device and service (routers, printers, NAS, IoT, admin consoles)			
2.2	Software that isn't needed has been removed (bloatware, trials, tools from old projects)			
2.3	Services and features that aren't needed are disabled			
2.4	User accounts that aren't needed have been removed or disabled — on devices AND in cloud services			
2.5	Autorun / autoplay is disabled (nothing executes just because media was inserted or a file arrived)			
2.6	Every device requires authentication to unlock: PIN of 6+ digits, password, or biometrics			
2.7	Brute-force protection is active: devices lock or throttle after repeated failed unlock attempts (e.g. max 10 guesses)			
2.8	Devices auto-lock after a short idle period			
2.9	Users authenticate individually before accessing business data — no shared, always-open sessions			
2.10	New devices are set up from a standard checklist or image, not from memory			
2.11	Key cloud services have been configured deliberately — sharing defaults reviewed, unused features off			
2.12	The device and cloud inventories in Part 1 are filled in and current			
	Control 2 total (/24)			

Evidence to collect now: your new-starter device setup checklist (write it if it doesn't exist — one page is fine); screenshots of screen-lock policy; the inventory tables from Part 1.

Quick wins: set a 6-digit-minimum PIN policy on phones today; uninstall software nobody has opened in six months; write the one-page setup checklist.

Control 3 — Security update management

What it demands. Everything in scope runs **licensed, vendor-supported** software. Automatic updates are on wherever possible. Vendor fixes for high or critical vulnerabilities (CVSS 7+) are applied within **14 days** — and "fixes" includes configuration changes and registry fixes the vendor issues, not just patch files. Unsupported software is removed, or formally segregated out of scope.

Why. The 14-day window isn't arbitrary: it's roughly how fast commodity exploitation follows public disclosure. Run unpatched for a month and you're not unlucky if you're hit — you're on schedule.

The five most common SMB failures:

1. One machine on an end-of-life OS — the automatic fail (see Part 1).
2. Updates technically enabled but endlessly deferred by users ("remind me tomorrow" for 90 days).
3. Browsers and Office updating, but the long tail — PDF readers, Zoom, drivers — forgotten.
4. Router and firewall **firmware** never updated since installation.
5. Nobody actually responsible: updates are everyone's job, so they're no one's.

Checklist 3 — Security update management

#	Item	Yes (2)	Partial (1)	No (0)
3.1	Every operating system in your inventory is still supported by its vendor			
3.2	All software is licensed and currently supported			
3.3	Unsupported software has been removed — or formally segregated so it's out of scope, with a dated plan			
3.4	OS automatic updates are enabled on every device			
3.5	Applications (browser, Office suite, the long tail) update automatically where they can			
3.6	High/critical vendor fixes (CVSS 7+) are applied within 14 days — including config-change fixes			
3.7	Router / firewall firmware gets updates, on the same 14-day clock for high/critical			
3.8	Phones and tablets in scope still receive OS security updates (no end-of-life Android/iOS)			
3.9	Someone (or something) would notice a critical patch announcement within days, not months			
3.10	Spot-check passed: pick 3 devices right now — all fully updated this month			
	Control 3 total (/20)			

Evidence to collect now: screenshots of update settings + "last updated" status on a device sample; firmware version vs vendor's latest for your router; the segregation plan for anything legacy.

Quick wins: run the 3-device spot-check today; set one calendar owner for "second Tuesday" patch review; check your router firmware (it's probably behind).

Control 4 — User access control

What it demands. Every person has their own account, created through an approval step and removed promptly when they leave. Admin rights live in **separate accounts used only for admin tasks**. MFA is enabled on every cloud service that offers it — non-negotiable for admins. Passwords are at least 8 characters with MFA (12 without), with no forced periodic expiry; passwordless methods (biometrics, security keys) are fine.

Why. Credentials are the modern break-in. Most "hacks" of small businesses are someone logging in with a stolen or guessed password — MFA alone defeats the overwhelming majority of those attempts. And admin-by-default means any single phished user hands over the entire business.

The five most common SMB failures:

1. MFA available on Microsoft 365 / Google Workspace but never enforced for everyone.
2. Everyone is a local admin on their own laptop.
3. The same account a director uses for daily email is also the global admin.
4. Leavers' accounts alive for months ("we might need their files" — archive the data, kill the account).
5. Shared logins for "the info@ inbox" or accounting software, password in a spreadsheet.

Checklist 4 — User access control

#	Item	Yes (2)	Partial (1)	No (0)
4.1	Every user has a unique account — no shared logins anywhere			
4.2	Creating an account requires an approval step (however lightweight), and it's recorded			
4.3	Leavers' accounts are disabled promptly — same week at the latest			
4.4	Accounts are reviewed periodically; unused ones get disabled			
4.5	Admin rights live in separate accounts from daily-use accounts			
4.6	Admin accounts are used ONLY for admin tasks — never email or browsing			
4.7	You hold a current list of who has admin rights on what			
4.8	MFA is enforced on EVERY cloud service that supports it — for all users			
4.9	MFA is enforced for every admin account, everywhere, no exceptions			
4.10	Password rules meet the scheme: 8+ chars with MFA, 12+ without; no forced periodic expiry; common-password deny-list where supported			
4.11	A password manager is available and people are encouraged to use it			
4.12	Legacy/basic authentication is disabled on cloud services where possible			
4.13	Third parties (contractors, your MSP) use their own named accounts, with MFA			
	Control 4 total (/26)			

Evidence to collect now: MFA enforcement report from M365/Workspace admin centre; the admin-rights list; your leaver-process note (a paragraph is fine — that it exists and is followed is the point).

Quick wins: enforce MFA tenant-wide this week (announce Friday, enforce Monday); strip local-admin from daily accounts; kill every shared login you can.

> **Instant-blocker check:** a cloud admin account without MFA is the single most consequential "No" in this workbook. If you fix one thing today, fix that.

Control 5 — Malware protection

What it demands. Every in-scope computer is protected by one of the two accepted mechanisms: **anti-malware software** (active, automatically updated, scanning on access, blocking known-malicious websites) or **application allow-listing** (only approved, signed applications can run). On phones and tablets, the practical route is official app stores only — no sideloading, no jailbroken or rooted devices touching business data.

Why. Malware is the payload stage of nearly every commodity attack — the phishing email, the poisoned download, the malicious ad all end in code trying to run on your device. This control decides whether it does.

The five most common SMB failures:

1. Relying on "we have Defender" without checking it's actually on, updating, and unbypassed on every machine.
2. Macs treated as immune — no protection, no allow-listing decision, nothing.
3. Users able to disable protection (and doing so when it "slows things down").
4. Android phones with sideloading enabled, or someone's old rooted device on business email.
5. Alerts going to a dashboard nobody opens.

Checklist 5 — Malware protection

#	Item	Yes (2)	Partial (1)	No (0)
5.1	Anti-malware is installed and ACTIVE on every in-scope Windows and macOS device (or allow-listing is properly in place — see 5.6)			
5.2	It updates automatically — engine and detections			
5.3	Real-time / on-access scanning is on (files checked when opened or downloaded)			
5.4	It blocks access to known-malicious websites			
5.5	Ordinary users cannot disable or bypass it			
5.6	If you use application allow-listing instead: only approved, signed applications run, from a maintained list			
5.7	Phones/tablets install apps from official stores only — sideloading and unknown sources are off			
5.8	No jailbroken or rooted devices access business data			
5.9	Email attachments and links are scanned (your M365/Workspace protections verified ON, not assumed)			
5.10	Someone sees and acts on malware alerts			
	Control 5 total (/20)			

Evidence to collect now: AV status across the fleet (your management console, or a screenshot sample); a phone settings screenshot showing unknown-sources off; where alerts land and who reads them.

Quick wins: verify Defender/XProtect status on every machine (10 minutes each); switch off "install unknown apps" on Android fleet; route alerts to an inbox a human reads.

Part 3 — Score, route, plan

3.1 Your scorecard

Copy your five control totals, then convert each to a percentage of its maximum:

Control	Your score	Max	%	Band
1 · Firewalls		20		
2 · Secure configuration		24		
3 · Security updates		20		
4 · User access control		26		
5 · Malware protection		20		
Overall		**110**		

Banding, per control: 🟢 90%+ · 🟡 60–89% · 🔴 below 60%

Your overall band is your weakest control's band. Cyber Essentials has no partial credit — every control must pass. One red control means a red overall, whatever the average says.

Override rule — instant blockers. Regardless of score, you are RED if any of these is true: any in-scope device on an unsupported OS · any cloud admin account without MFA · any default password still in place on an internet-facing device.

3.2 What your band means

🟢 **Green — Ready.** You're substantively there. Buy the official question set process directly: pick a certification body via IASME, answer the questions using the evidence you collected here, get board sign-off, submit. Expect the verification to surface a handful of wording-level gaps — your evidence pack handles them. Realistic timeline: **1–2 weeks**, mostly admin.

🟡 **Amber — Nearly.** The typical SMB position: fundamentals present, enforcement patchy ("most devices", "most users" — the scheme requires *all*). Work the remediation planner below; the quick wins in each chapter are designed to move exactly these scores, and Appendix A shows you how to verify each fix. Realistic timeline: **2–6 weeks** depending on device count and how much is centrally manageable. Most businesses in this band close the gaps themselves.

🔴 **Red — Gaps.** Usually one of: end-of-life systems still in service, no MFA culture, or no inventory (so no one knows what's true). Don't attempt certification yet — you'd be paying to fail. Fix the instant blockers first, then re-run Part 2. Realistic timeline: **4–8+ weeks**. Take the structural decisions (replace vs retire vs segregate, tooling) deliberately — wrong turns there are where most time and money get lost, and they're the right questions to get a second opinion on, whoever you ask.

3.3 Remediation planner

Pre-seeded with the ten fixes that come up in almost every SMB assessment — delete what doesn't apply, add your own from every Partial/No above:

#	Fix	Control	Owner	Effort	Target date	Done
1	Enforce MFA on all cloud services, all users	4		S		☐
2	Replace/retire/segregate unsupported OS devices	3		M–L		☐
3	Change default router/admin passwords	1+2		S		☐
4	Turn on software firewalls fleet-wide (incl. Macs)	1		S		☐
5	Separate admin accounts from daily accounts	4		M		☐
6	Enable auto-updates everywhere; assign a patch owner	3		S		☐
7	Verify anti-malware active + auto-updating on every device	5		S		☐
8	Set device unlock policy (6+ digit PIN / biometrics + lockout)	2		S		☐
9	Disable leavers' accounts; review all accounts quarterly	4		S		☐
10	Close unjustified port forwards; disable UPnP	1		S		☐
11						☐
12						☐

Sequence by blast radius, not by ease: instant blockers → MFA → updates/EOL → access control → the rest. (It's tempting to do the easy ones first. Do the ones that stop a breach first.)

3.4 The 2–6 week path, week by week

What a typical Cyber Essentials run looks like for a 5–50 person business:

- **Week 1 — Scope & evidence.** Confirm the boundary, complete inventories, identify blockers. Decisions: whole-org vs sub-set, replace vs segregate for anything legacy. *(You've done ~70% of this by finishing the workbook.)*
- **Weeks 2–3 — Fix sprint.** MFA enforcement, update posture, access-control cleanup, configuration baselines. Central tooling (M365/Workspace policies, MDM) does the heavy lifting; stragglers get handled device-by-device.
- **Week 4 — Evidence pack & dry run.** Answer the official question set as a rehearsal against your evidence; close the wording-level gaps that surface.
- **Weeks 5–6 — Submission.** Final answers in, board-member declaration signed, assessor verification handled, certificate issued. (CE Plus, if required: the audit must follow within three months — book it now while everything's fresh.)

A realistic note on pace: everything in this workbook is doable in-house — that's the point of it. Just budget honestly: the *working* time is days, but the *elapsed* time is usually weeks, because these tasks compete with running your actual business. Put the dates in the planner, give each fix an owner, and treat the 14-day patch rule as the rhythm the whole thing runs on. If a contract deadline is forcing the pace, getting help is sensible — any reputable consultant should work to a fixed scope that you control, and your certification body can point you to suitable support.

Appendix

A. How to check — the ten most-failed items

You don't need to be technical to verify most of this workbook. Here is exactly where to look for the checks SMBs most often get wrong. (Menus move around between versions — if a path doesn't match, search the setting name.)

1. **Is MFA actually enforced — not just available?** Microsoft 365: admin centre → Users → Active users → *Multi-factor authentication* (or Entra admin centre → check Security Defaults / Conditional Access). Google Workspace: Admin console → Security → Authentication → 2-step verification → confirm **Enforcement**, not just "allowed". Real-world test: ask two colleagues to sign in on a fresh browser — were they asked for a second factor?
2. **Is the firewall on?** Windows: Start → type "Windows Security" → *Firewall & network protection* — all three network types should say **On**. macOS: System Settings → Network → Firewall — it ships **off**; turn it on.
3. **Is this computer's operating system still supported?** Windows: press Win+R, type `winver`, note the version — then search "Windows lifecycle" and check it against Microsoft's dates. macOS: Apple ships security updates for roughly the current and two previous versions — anything older, plan the upgrade.
4. **Has the router's admin password been changed?** If the admin password is still the one printed on the router's sticker, it hasn't. Browse to the router (commonly 192.168.0.1 or 192.168.1.1), sign in, change it — and note it in your password manager.
5. **What's exposed to the internet?** In the router's admin pages, find *Port forwarding* / *NAT* / *Virtual servers*. Every entry should have a reason you can say out loud. Delete the ones you can't explain, and switch **UPnP off** while you're there.
6. **Are updates actually automatic?** Windows: Settings → Windows Update — "You're up to date", and *last checked* within days. macOS: System Settings → General → Software Update → Automatic updates **on**. Then spot-check one laptop that's been on holiday with its owner — that's the one that's behind.
7. **Who is an admin?** Windows: Settings → Accounts → Other users — who's an Administrator? Microsoft 365: admin centre → Users → filter by admin roles. The list should be short, current, and contain no daily-use accounts.
8. **Is the screen lock real?** Windows: Settings → Accounts → Sign-in options (require sign-in on wake). iPhone: Settings → Face ID & Passcode — passcode set, 6 digits. Android: Settings → Security → Screen lock.
9. **Can apps be installed from outside official stores?** Android: Settings → Apps → Special app access → *Install unknown apps* — everything should say **Not allowed**. iPhone: not possible by default — just don't install configuration profiles you don't recognise.
10. **Is anti-malware on and current?** Windows: Windows Security → *Virus & threat protection* — protection on, definitions current, last scan recent. macOS: built-in protection (XProtect) runs automatically; if you've added a third-party product, open it and check its status and last update — and that an ordinary user can't just switch it off.

B. Glossary — plain English

- **Boundary firewall** — the barrier between your network and the internet, usually inside your router.
- **BYOD** — Bring Your Own Device; personal phones/laptops used for work. In scope.
- **CVSS** — a 0–10 severity score for vulnerabilities. 7+ means high/critical → your 14-day clock.
- **End of life (EOL)** — the vendor has stopped shipping security fixes. EOL in scope = automatic fail.
- **Legacy authentication** — older sign-in methods that bypass MFA. Disable where possible.
- **MFA** — multi-factor authentication; a second proof (app prompt, code, security key) beyond the password.
- **Sideloading** — installing mobile apps from outside official stores. Off, for business devices.
- **Segregation** — genuinely separating a system from your network so it can sit outside scope (a VLAN with no access to business data, not just "a different Wi-Fi name").

C. Official resources

- **NCSC — Cyber Essentials overview:** ncsc.gov.uk/cyberessentials
- **IASME (delivery partner)** — question set download, certification bodies, current fees: iasme.co.uk
- **NCSC Requirements for IT Infrastructure** — the authoritative control definitions (free PDF via the NCSC CE pages)
- The official **readiness toolkit** on the NCSC site complements this workbook with the scheme's own question phrasing.

D. About this workbook

Written by **Hemanth Vishnu Akula** — ISO 27001:2022 Lead Auditor and fractional vCISO — because most SMBs can get certification-ready themselves with a clear map, and deserve one that isn't behind an email wall. If you'd like a second pair of eyes on your scorecard, or help with the journey, you can reach me at **hemanthvishnuakula.com/contact**. Separately: whatever you decide about certification, it's worth checking your email security — **authexlabs.com/scanner** is a free 30-second scan of your domain's trust layer.

Cyber Essentials Readiness Workbook · v1.1 · June 2026 Written against the Cyber Essentials **"Willow" question set (v3.2)** and the corresponding NCSC Requirements for IT Infrastructure. The scheme updates periodically — if a newer question set is in force when you read this, check iasme.co.uk and treat the official documents as authoritative. Canonical version: **hemanthvishnuakula.com/resources**