TRANSCRYPT

From Panic to Prepared: Your 90-Day Cyber Essentials Roadmap

You've just been told you need Cyber Essentials certification. Maybe it's for a contract renewal, an insurance requirement, or a client who won't budge. Whatever the reason, you're now facing a deadline and a certification process you don't fully understand.

Take a breath. Ninety days is enough.

This guide breaks the journey from "where do I even start?" to "certification achieved" into manageable weekly sprints. No prior technical knowledge required. No expensive consultants necessary. Just a clear path forward.

Before You Begin: The Reality Check

First, let's be honest about what you're facing. Cyber Essentials isn't a single afternoon's work, but it's not building the Pyramids either. Most small businesses need between 20-40 hours of actual effort spread across three months. That's roughly 2-4 hours per week—completely manageable alongside running your business.

The certification covers five control areas: firewalls, secure configuration, access control, malware protection, and patch management. If those terms make your eyes glaze over, that's fine. By the end of this guide, you'll understand exactly what they mean for your business.

What you'll need:

- Admin access to your computers, routers, and any cloud services
- Authority to make changes to company devices and accounts
- About 3-4 hours per week for the next 90 days
- Willingness to ask "stupid" questions (there aren't any)

Week 1-2: Discovery and Assessment

Your mission: Understand what you're actually certifying.

The biggest mistake businesses make is diving straight into "fixing" things without knowing what needs fixing. Start with a proper stocktake.

Create your asset inventory. Make a simple spreadsheet listing every device that touches company data: laptops, desktops, phones, tablets, servers. Include the operating system (Windows 11, macOS Ventura, etc.) and who uses it. This isn't a box-ticking exercise—you can't protect what you don't know exists.

Map your network boundaries. Where does your business network start and end? Do you have a physical office with a router? Do staff work from home? Are you entirely cloud-based? Sketch it out, even if it's just boxes and arrows on paper. Understanding your digital footprint is half the battle.

Identify your IT decision-maker. This might be you, an external IT provider, or "Dave who's good with computers." You need to know who has the authority and ability to make technical changes, because you'll need them in the next phase.

Baseline assessment. Go through each device and note the basics: Is antivirus installed and running? Is Windows Update turned on? Do people use the same password for everything? Are company laptops and personal laptops mixed together? You're not fixing anything yet—just documenting reality without judgment.

Time investment: 4-6 hours across two weeks

Common pitfall: Discovering you don't actually have admin access to critical systems. Chase down credentials now, not in week ten.

Week 3-5: Quick Wins and Low-Hanging Fruit

Your mission: Implement the changes that take minimal effort but maximum impact.

Now you know what you're working with, it's time for the easy victories that dramatically improve your security posture.

Enable automatic updates everywhere. This single action addresses the patch management control. Windows Update, macOS Software Update, app auto-updates—turn them all on. Yes, updates occasionally cause hiccups. Security breaches definitely cause hiccups. Configure updates to install overnight if you're worried about disruption.

Deploy proper antivirus/endpoint protection. If you're relying on whatever came free with Windows, upgrade to business-grade protection. Products like Microsoft Defender for Business, Bitdefender, or ESET cost less than your weekly coffee budget and handle the malware protection control comprehensively. Install it everywhere, ensure it's updating automatically, and verify it's actually scanning.

Audit user accounts. Go through every system and remove accounts for people who've left, contractors whose projects finished, or that "test" account someone created three years ago. Every unnecessary account is a door you've left unlocked. This begins addressing the access control requirement.

Enable basic firewalls. Windows Firewall, macOS Firewall—they're already on your devices, probably switched off. Turn them on. If you have a physical office, log into your router and verify its firewall is active. This isn't sophisticated network security; it's pulling up the drawbridge.

Document everything. Screenshot every settings page, keep a log of what you've changed, photograph the back of your router if needed. Evidence is currency in the certification process. Assume you'll need to prove every action you've taken.

Time investment: 8-12 hours across three weeks

Common pitfall: Fixing things without recording what you did. An auditor doesn't care that you've configured something correctly if you can't prove it.

Week 6-8: The Hard Yards

Your mission: Tackle the configuration issues that require thought and potentially cost.

This is where most businesses hit resistance, because now you're dealing with inconvenient truths about how you actually operate versus how you should operate.

Address unsupported software. Still running Windows 7? Office 2013? That ancient accounting package that "still works fine"? Unsupported software is certification poison. You have three options: upgrade it, replace it, or isolate it from your network (which is complex and probably not worth it). Make the decision now, because implementation takes time.

Implement proper password controls. Cyber Essentials requires password complexity and management. This means enabling password requirements on all devices (minimum 12 characters, ideally), deploying a password manager across the business, and removing shared accounts. Yes, people will complain. Yes, it's necessary. Communicate why it matters: every shared password is a liability you're all carrying.

Separate admin and standard accounts. Staff shouldn't be working with administrator privileges day-to-day—it's the digital equivalent of driving while wearing a blindfold. Create standard user accounts for daily work and separate admin accounts for when you actually need elevated permissions. This feels like overkill until you consider that most malware relies on users accidentally running malicious code with full system access.

Configure secure settings on devices. This varies by platform, but the principle is consistent: turn off unnecessary services, disable auto-run features, require authentication to wake from sleep, enable disk encryption. The secure configuration control is about reducing your attack surface. If you don't need a feature, switch it off.

Cloud service audit. List every cloud service your business uses: email, file storage, CRM, accounting. Verify each has multi-factor authentication enabled, check who has access, remove old integrations and unused apps. Cloud services are computers too—they just happen to be someone else's computers.

Time investment: 10-15 hours across three weeks

Common pitfall: Getting bogged down in perfection. You're aiming for "secure enough to certify," not "impervious to nation-state actors." Progress over perfection.

Week 9-10: Documentation and Policy

Your mission: Create the written policies that demonstrate you've thought about security, not just implemented it.

Cyber Essentials requires written policies that govern how you handle security. These don't need to be fifty-page epics—clear, concise, and actually followed beats comprehensive and ignored.

Essential policies you need:

- **Acceptable Use Policy:** What's acceptable and unacceptable use of company IT equipment and services
- **Password Policy:** Requirements for password strength, storage, and changing
- **BYOD Policy** (if applicable): Rules for personal devices accessing company data
- **Access Control Policy:** How you grant, review, and revoke system access
- **Remote Working Policy** (if applicable): Security expectations for working outside the office

Each policy needs three elements: what the rule is, why it exists, and what happens if someone breaks it. Keep the language simple—you're writing for your team, not lawyers.

The authenticity test: Could you hand this policy to a new employee and have them actually follow it? If not, rewrite it. Policies that don't reflect reality are worse than useless—they demonstrate to auditors that you don't take your own rules seriously.

Time investment: 6-8 hours across two weeks

Common pitfall: Copying policies from the internet verbatim. Auditors spot this instantly, and it raises questions about whether you understand or enforce what you've written.

Week 11: Evidence Gathering and Internal Audit

Your mission: Assemble everything an auditor will want to see.

By now, you've done the work. Week eleven is about proving it.

Create your evidence pack:

- Screenshots of security settings on representative devices
- Logs from antivirus showing it's running and up-to-date
- List of user accounts showing proper access control
- Network diagram showing your firewall setup
- Copies of all policies, ideally with evidence they've been communicated to staff
- Asset inventory showing all devices are accounted for

Conduct your own mini-audit. Pick one device at random and verify everything you think you've configured is actually in place. Then pick another. You're looking for gaps between "we configured this" and "it's still configured." Settings revert, updates fail silently, and staff work around controls they find inconvenient. Better you discover these issues than an external auditor.

Address the gaps. Whatever you find, fix it now. Then update your evidence pack to reflect the reality.

Time investment: 4-6 hours

Common pitfall: Assuming everything you configured weeks ago is still configured. Trust, but verify.

Week 12: Certification Application

Your mission: Submit your assessment and pass.

You're ready. You've done the work, gathered the evidence, and verified it's all in place. Time to make it official.

Choose your certification body. Several IASME-accredited bodies offer Cyber Essentials certification. They're not all identical—prices vary (typically £300-500 for basic Cyber Essentials), as does the assessment experience. Read recent reviews, check turnaround times.

Complete the self-assessment questionnaire. This is the formal bit: a detailed form asking about your implementation of each control. Be honest and precise. If you've followed this roadmap, you'll have clear answers for every question. Where you're asked for evidence, you'll know exactly which document or screenshot to provide.

Submit and wait. The certification body reviews your submission, may ask clarifying questions, and issues your certificate if you've met the requirements. Turnaround varies from a few days to a few weeks depending on the body and time of year.

Time investment: 3-4 hours

If you don't pass: Don't panic. Failed first assessments are common, usually due to small gaps in evidence or minor misconfigurations. The certification body will tell you exactly what needs addressing. Fix it, resubmit. Most businesses pass on the second attempt.

After Certification: Staying Compliant

Getting certified is the beginning, not the end. Cyber Essentials is valid for twelve months, after which you'll need to renew. The businesses that find renewal effortless are those that maintain compliance year-round rather than treating it as an annual sprint.

Build compliance into your rhythm:

- Monthly: Quick check that antivirus and updates are still running across all devices
- Quarterly: Review user accounts and remove any that are no longer needed
- When someone joins or leaves: Update access controls immediately
- When you buy new equipment or software: Ensure it's configured securely from day one

Think of certification like an MOT for your business. The garage checks your car is roadworthy, but you don't then ignore maintenance for twelve months. Same principle applies here.

The Bottom Line

Ninety days from now, you'll have a certificate that opens doors to contracts, satisfies insurers, and demonstrates to clients that you take security seriously. More importantly, you'll actually be more secure—not because you've spent a fortune on enterprise tools, but because you've implemented sensible, proportionate controls that suit your business.

The journey from panic to prepared isn't about becoming a cyber security expert. It's about being methodical, honest about your current state, and willing to make changes that might occasionally inconvenience people but ultimately protect everyone.

You've got this. Week one starts now.