The Essential UK SME Guide:

Cyber Essentials Self-Assessment & Readiness Checklist

Introduction

In the UK's competitive digital landscape, Cyber Essentials (CE) isn't just a desirable certification—it's often a prerequisite for government contracts and a clear signal of trust to your customers.

This guide has been created by **Fortitude Cyber** specifically for UK SMEs. It serves as a practical, actionable roadmap to help you understand the five core Cyber Essentials control areas, assess your current security readiness, and identify the most common pitfalls that lead to certification failure.

By the end of this self-assessment, you will have a clear picture of your security posture and the steps required to achieve compliance, protect your business, and secure new opportunities.

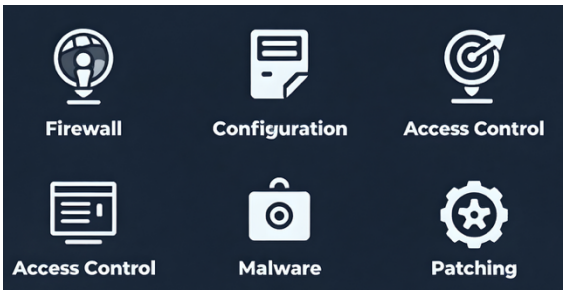
⚠️ The 12 Most Common Reasons SMEs Fail Cyber Essentials

Certification auditors consistently see the same security gaps trip up small and medium-sized businesses. Knowing these issues in advance is the first step toward a successful outcome.

Failure Point	Risk & Impact
Unsupported Operating Systems	Running OS versions (e.g., old Windows/macOS) that no longer receive security patches leaves your systems perpetually vulnerable to known exploits.

Failure Point	Risk & Impact
Missing Security Updates	Patches are available but haven't been applied within the required **14 days**. This is the single biggest opening for opportunistic cybercriminals.
Weak or Reused Passwords	Using simple, dictionary-based passwords or reusing the same password across multiple services makes your entire business vulnerable if one account is compromised.
MFA Not Enforced for Remote Access	Multi-Factor Authentication (MFA) is a mandatory requirement for any access to the organization's data or services from outside the network.
No Device Inventory	You cannot secure what you do not know about. An incomplete or missing list of all in-scope devices (laptops, phones, servers) makes compliance impossible.
Unencrypted Mobile Devices	Laptops, tablets, and smartphones that hold company data must have hard-disk encryption enabled (e.g., BitLocker, FileVault) to protect data in the event of loss or theft.
Inconsistent Antivirus/EDR Deployment	Not all devices have up-to-date anti-malware software installed, or the solution is not centrally managed and monitored.
Missing Firewall Rules or Open Ports	Having unnecessary ports open to the public internet (e.g., RDP, FTP) provides direct, unmonitored access to your internal network.
Admin Accounts Used for Day-to-Day Tasks	Using highly privileged administrator accounts for daily activities like web browsing or email exposes the business to unnecessary risk from phishing and malware.
No Backup Testing	The existence of a backup is meaningless if the process to *restore* data has never been successfully tested and documented.
No Patching Process	While updates may be applied, there is no formal, documented process to ensure every device is checked and updated on a regular, consistent basis.
Missing or Outdated Policies	Security policies (e.g., acceptable use, password) are either non-existent or haven't been communicated to staff, meaning security measures are inconsistent.

🔎 Checklist by Control Area: The Five Cyber Essentials Controls



To achieve certification, you must demonstrate competence across all five technical control areas. Use this section to check your current status.

1. FIREWALLS

- **Purpose:** To create a digital barrier that prevents unauthorized access to your devices and network.
- **Key Questions:**
  - ✅ **Is every in-scope device (desktop, laptop, server) protected by a firewall?**(This can be a hardware firewall or a software/OS firewall.)
  - ✅ **Have the default administrative passwords on your router and firewall been changed to something unique and strong?**
  - ✅ **Are all unnecessary inbound ports closed off to the public internet?** (Only essential services like web/email traffic should be permitted.)

2. SECURE CONFIGURATION

- **Purpose:** To ensure your devices are configured in the safest possible way, removing unnecessary functionality that could be exploited.
- **Key Questions:**
  - ✅ **Is all unused software and unnecessary functionality (e.g., development tools, default accounts) removed from all in-scope devices?**
  - ✅ **Is Multi-Factor Authentication (MFA) enforced for all administrator and user accounts that can access cloud services or corporate data remotely?**
  - ✅ **Are system defaults (e.g., "Guest" accounts) disabled, and have secure password policies been applied at the operating system level?**

3. USER ACCESS CONTROL

- **Purpose:** To ensure only authorized users can access the data and services they require, using the principle of **least privilege**.
- **Key Questions:**
  - ✅ **Do you have a robust, enforced strong password policy?** (E.g., minimum length of 10 characters for user accounts, or a minimum length of 8 characters if enforced with MFA.)
  - ✅ **Are administrator/highly privileged accounts separate from day-to-day user accounts?** (Staff should use their standard account for email/browsing.)
  - ✅ **Do you have a defined Joiner/Mover/Leaver process to ensure accounts are created securely and access is revoked immediately upon departure?**

4. MALWARE PROTECTION

- **Purpose:** To protect your devices from infection by malicious software such as viruses, ransomware, and spyware.
- **Key Questions:**
  - ✅ **Is next-generation anti-malware (Antivirus/EDR) installed and operational on *all* devices in scope?**
  - ✅ **Is real-time (on-access) scanning enabled and running continuously on all devices?**
  - ✅ **Are malware definitions updating automatically, and have all staff been trained *not* to disable the protection?**

5. PATCH MANAGEMENT

- **Purpose:** To ensure that all operating systems and software are kept up to date to close known security vulnerabilities.
- **Key Questions:**
  - ✅ **Are all operating systems (Windows, macOS, Linux, firmware) and key applications (web browsers, productivity suites) currently supported by the vendor?**
  - ✅ **Are security updates and patches applied to all in-scope devices within 14 days of their release?**
  - ✅ **Is your patching process documented and centrally monitored to ensure no device is missed?**

📋 What Auditors Actually Look For: Proof, Not Promises

Auditors cannot simply take your word for it. They are looking for **clear, undeniable evidence** that your controls are consistently implemented across the entire scope of the assessment.

Be prepared to provide:

- **System Evidence:** Screenshots of firewall settings, encryption confirmation pages, and secure configuration settings (e.g., password policies).
- **Device Inventory:** A complete and accurate list of all devices, including the operating system and installed anti-malware status.
- **Policy Documentation:** Copies of your Acceptable Use, Password, and Patching policies.
- **Access Control Records:** Logs and screenshots showing that MFA is enabled and how privileged access is controlled.
- **Update Logs:** Evidence showing that critical and high-priority updates have been applied promptly.

✅ Self-Assessment Scoring Template

Rate your current implementation status for each of the 15 control-area questions above.

Score	Status	Description
0	**Not Implemented**	The requirement is not in place at all, or implementation is inconsistent.
1	**Partially Implemented**	The requirement is in place, but requires significant documentation, consistency, or coverage improvements.
2	**Fully Implemented**	The requirement is consistently in place across all devices and is fully documented.

Total Your Readiness:

Total Score	Readiness Level	Next Step
0–10	**High Risk of CE Failure**	Significant foundational work required. Prioritise Quick Fixes immediately.
11–20	**Needs Improvement**	A solid foundation exists, but inconsistent application or missing policies will likely cause failure.
21–30	**Likely to Pass with Minor Fixes**	You are close! Focus on gathering evidence and formalizing your policies.

🛠️ Actionable Quick Wins: Low-Cost Fixes (£0–£50)

Many major security improvements require minimal financial outlay. Here are simple, high-impact changes you can implement today:

- **Enable MFA Everywhere:** Use free MFA apps (like Google Authenticator or Microsoft Authenticator) to protect all cloud services (Microsoft 365, Google Workspace, CRM, HR portals).
- **Decommission Unused Accounts:** Conduct a user audit and remove all accounts for past employees or services that are no longer in use.
- **Enforce Strong Passwords:** Use a free password manager and set a clear, minimum 10-character password length policy for all staff.
- **Enable Automatic Updates:** Ensure all operating systems (Windows Update, macOS App Store) are set to install updates automatically, especially outside of business hours.
- **Turn on Device Encryption:** Use the built-in encryption features of your OS (BitLocker for Windows Pro, FileVault for macOS) on all laptops and desktops storing company data.

➡️ Next Steps: Get Certified with Fortitude Cyber

You've completed the first step toward a successful certification. Now, let our experts guide you to the finish line.

The final stage of certification involves translating your technical controls into the evidence auditors require.

Book a free, no-obligation readiness review at fortitudecyber.co.uk today.

We will walk through your self-assessment results with you, pinpoint your specific vulnerabilities, and discuss a tailored, fixed-price action plan to ensure you achieve Cyber Essentials certification quickly and efficiently.