CYBERGEN®

28th, August 2025

Accelerating Cyber Essentials Plus Readiness for SMEs

Produced by:
Aaron Bennett

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS PLUS

Executive Summary

Cyber threats are increasing in both frequency and sophistication, and small to medium-sized enterprises (SMEs) are becoming attractive targets for attackers. Achieving Cyber Essentials Plus certification is a key step in strengthening cyber defences and demonstrating a commitment to security. However, for many SMEs, navigating the certification process can be a daunting task.

This ebook offers a practical, step-by-step guide to accelerating readiness for Cyber Essentials Plus. Drawing from Cybergen's consultancy expertise, we provide actionable insights, templates, and real-world examples to help SMEs achieve certification efficiently and sustainably.

1. Understanding Cyber Essentials Plus

1.1 What is Cyber Essentials Plus?

Cyber Essentials Plus is a UK Government-backed cyber security certification scheme that helps organisations protect themselves against common online threats. While the basic Cyber Essentials certification involves a self-assessment, Cyber Essentials Plus goes further by requiring an independent technical audit.

- Overview of the UK Government-backed scheme: Administered by the National Cyber Security Centre (NCSC) and overseen by IASME, the scheme outlines key controls organisations must implement to guard against the most common cyber threats.
- Difference between Cyber Essentials and Cyber Essentials Plus: Cyber Essentials is a self-assessment certification, while Cyber Essentials Plus involves a more rigorous audit conducted by a qualified assessor. The Plus certification verifies that the security controls are properly implemented and effective in a real-world environment.

Benefits:

- **Reduced cyber risk:** Implementation of core controls significantly decreases the likelihood of common attacks like phishing, malware, and ransomware.
- **Enhanced customer trust:** Certification demonstrates commitment to cybersecurity, improving confidence among customers and partners.
- **Eligibility for certain contracts:** Particularly for government and defence supply chain contracts, Cyber Essentials Plus is often a mandatory requirement.

> "Small businesses are not just targets, they're the preferred targets. Over 50% of cyber attacks are aimed at SMEs, who often lack the robust defences of larger enterprises."
> — National Cyber Security Centre (NCSC), UK

1.2 Why SMEs Should Prioritise Certification

SMEs are frequently targeted by cybercriminals due to often limited defences and under-resourced IT teams. Certification offers protection and a competitive edge.

- Demonstrated Commitment to Cyber Security
- Protection Against Common Threats
- Independent Verification
- Enhanced Business Reputation
- Eligibility for Government Contracts
- Stronger Supply Chain Position
- Cost-Effective Security Baseline
- A Foundation for Further Accreditation

2. Common Pitfalls and How to Avoid Them

2.1 Importance of Defining the Correct Scope

Under Cyber Essentials Plus, the scope must include all in-scope devices, applications, and users that access business data—especially those connected to the internet. SMEs often misunderstand or narrow their scope, excluding remote workers, cloud services, or mobile devices, which leads to non-compliance.

A clear, accurate scope ensures that all systems are subject to the five Cyber Essentials control areas: firewalls, secure configuration, access control, malware protection, and patch management.

Example of Poor Scoping and Its Impact

An SME included only office desktops in its CE+ assessment and excluded remote laptops used by employees working from home. One of these laptops, which lacked patching and anti-malware protection, was compromised, leading to a ransomware infection. The company failed its CE+ reassessment, incurring additional consultancy and testing costs, and experienced downtime that impacted its clients.

2.2 Inadequate Patch Management

Requirements for Patching Timescales (CE+ Specific)

Cyber Essentials Plus requires that all high and critical security updates be applied within 14 days of release. This applies to operating systems, third-party applications, firmware, and internet-facing services.
Tools and Practices to Stay Compliant

- Recommended Tools for SMEs: Microsoft Intune (for Windows devices), N-able, NinjaOne, and Patch My PC. These are scalable and cost-effective.

Best Practices for your business

- Enable automatic updates where feasible.
- Maintain a patch register with evidence of updates applied.
- Regularly run vulnerability scans (e.g., using Nessus or Qualys) to ensure no missing patches.
- Document patching policies and assign clear responsibilities.

2.3 Weak Access Controls

Misconfigurations in User Accounts
CE+ assessments often reveal issues such as:

- Shared administrator accounts without auditing.
- User accounts with local admin privileges by default.
- Dormant or former employee accounts still active.

These pose serious risks and will result in CE+ test failure.

Importance of Multi-Factor Authentication (MFA)
Cyber Essentials requires MFA for:

All cloud services (e.g., Microsoft 365, Google Workspace).

- Administrator-level accounts.
- SMEs should enforce MFA using tools like Microsoft Authenticator or Google Authenticator and ensure it's tested during the CE+ audit.

2.4 Poorly Maintained Asset Inventory

Keeping an Up-to-Date Asset Register

An accurate asset register helps ensure that only authorised, supported, and secure devices are connected to the business network. CE+ requires visibility over all endpoints included in scope, including mobile devices and home-working laptops.

Tools to Assist Asset Management for SMEs

- **Low-cost solutions:** Spiceworks, Lansweeper (free tier), or device inventory in Microsoft Intune.

- **Best Practices:**
  - Maintain a live register of laptops, desktops, smartphones, and software in use.
  - Ensure any new devices are configured securely before deployment.
  - Decommission and wipe retired devices promptly.

2.5 Neglecting Mobile and Remote Working Devices

Devices such as Laptops, Smartphones, and Home Networks in the Scope for CE+ require that all devices connecting to the business environment, regardless of location, are within scope. This includes:

- Work laptops are used at home or in the field.
- Employee-owned smartphones (if used for work email or apps).
- Devices accessing business systems over home Wi-Fi.

Failure to account for these can cause test failure and leave exploitable gaps.
Secure Configuration and Monitoring

- **Configuration Requirements:**
  - Full disk encryption (BitLocker, FileVault).
  - Auto-lock after inactivity.
  - Disabled admin access for standard users.

- **Monitoring Tools:**
  - MDM solutions such as Microsoft Intune, Jamf (for Apple), or Kandji.
  - Remote wipe capability.
  - Endpoint antivirus/EDR with reporting.

3.0 Fast-Track Compliance: Toolkit

Identifying Current State vs. Cyber Essentials Plus Requirements
Gap analysis helps SMEs map their existing cybersecurity posture against CE+ requirements. This process highlights areas of non-compliance and prioritises remediation efforts before assessment.

Key areas for comparison:

- Boundary firewalls and internet gateways
- Secure configuration
- User access control
- Malware protection
- Security update management

Sample Gap Analysis Spreadsheet

Control Area	Current State	CE+ Requirement	Gap Identified	Action Required	Owner	Target Date
User Access Control	All staff use same admin credentials	Unique accounts, least privilege	Shared accounts in use	Implement unique admin accounts	IT Lead	1 Sept 20...
Malware Protection	Free AV on some machines	Must be centrally managed and up to date	Inconsistent AV deployment	Deploy centralized endpoint protection	IT Team	15 Sept 2...
Patch Management	Ad hoc patching, no central control	High-risk updates within 14 days	No formal patching process	Set up automated patch management	SysAdmin	10 Sept 2...

3.2 Policy Templates

Cyber Essentials Plus requires clear, documented policies to support technical controls. SMEs can adapt the following templates:

The below is what you need:

- **Password Policy:**

Enforce minimum length (12+ characters), complexity, and MFA. **Ban reuse and ensure regular password audits.**

- **Patch Management Policy:**

Define timeframes (e.g., 14 days for high/critical patches), responsible roles, tools used, and documentation requirements.

- **Access Control Policy:**

Enforce least privilege, account provisioning and de-provisioning, and periodic access reviews.

3.3 Checklist for Internal Audit Preparation

Technical Controls Checklist:

- ☐ Firewalls configured to block unauthorised inbound traffic
- ☐ Default admin passwords changed
- ☐ Only necessary software/services installed
- ☐ Automatic updates enabled and monitored
- ☐ Endpoint protection is deployed and centrally managed
- ☐ MFA enabled on all cloud and remote access
- ☐ All devices are listed in the asset register

Physical Security Considerations:

- ☐ Office has secure entry (e.g., badge or PIN access)
- ☐ Server rooms locked or restricted
- ☐ Visitor log maintained (if applicable)
- ☐ Backup devices (e.g., USBs) secured or encrypted
- ☐ Devices are locked when unattended

The above checklist can be used as a pre-assessment tool to ensure readiness for the CE+ audit.

3.4 Toolkits and Automation

Recommended Tools (affordable and SME-friendly):

- **Vulnerability Scanning:** Nessus Essentials, Qualys
- **Patching:** Microsoft Intune
- **Endpoint Protection:** WatchGuard, Sophos Central, Microsoft Defender for Business.

Benefits of Automation:

- Reduced human error in patching and updates
- Faster threat detection and response
- Scalable security posture without increasing headcount
- Real-time compliance tracking and alerting

Are you ready for Cyber Essential Plus?

Define the Assessment Scope

- Identify and document all devices, users, and applications that access company data.
- Include remote workers, mobile devices, and cloud services (e.g., Microsoft 365, Google Workspace).
- Ensure no critical systems are excluded without justification.

Firewalls and Internet Gateways

- Ensure firewalls are enabled on all devices (hardware and software).
- Restrict inbound traffic to only what is essential (e.g., no open RDP or SSH from the internet).
- Change default admin passwords on routers and firewalls.

Secure Configuration

- Remove or disable unnecessary user accounts, services, and applications.
- Disable AutoRun and macro settings in Office files by default.
- Ensure devices auto-lock after 10 minutes or less of inactivity.
- Prevent users from running executables from temp or downloads folders.

User Access Control

- Create unique accounts for all users (no shared logins).
- Enforce least privilege, **no admin rights for standard users.**
- Disable or delete old user accounts promptly when staff leave.

Use Multi-Factor Authentication (MFA) for:

- All remote/cloud services
- Admin accounts

Malware Protection

- Install centrally managed anti-malware/endpoint protection on all devices.
- Ensure real-time scanning and automatic updates are enabled.
- Avoid using free or unmanaged antivirus software.
- Block access to known malicious websites (web filtering, if available).

Patch Management

- Apply security updates within 14 days of release for:
- Operating systems
- Applications
- Firmware (e.g., routers)
- Use automated patching tools where possible (e.g., Intune, WSUS).
- Keep unsupported software (e.g., old Windows versions) off your systems.

Maintain an Asset Inventory

- Keep a live register of all:
- Laptops/desktops
- Mobile devices
- Software and cloud services
- Regularly review and update the inventory.

Prepare for the CE+ Audit

- Run a vulnerability scan across all in-scope systems.
- Perform an internal audit using a CE+ checklist.
- Fix any identified gaps (missing patches, weak passwords, firewall issues).
- Test MFA and ensure it works on all required systems.
- Verify antivirus and updates are active and functioning.

Backup and Recovery (Best Practice – not required for CE+)

- While not part of CE+, it's strongly advised to:
- Regularly back up business-critical data
- Store backups offline or offsite
- Test restore procedures

Document Supporting Policies

Maintain and review:

- Access Control Policy
- Password Policy
- Patch Management Policy
- Bring Your Own Device (BYOD) Policy

Assign roles/responsibilities for compliance.

Need help with Cyber Essentials? Schedule a session with our experts today and take the next step toward certification.

sales@cybergensecurity.co.uk +44 (0) 1865 950 828 www.cybergensecurity.co.uk

Join Our Social Community