Cloudswitched | Cyber Security

FREE RESOURCE — GUIDE

Cyber Essentials Plus Preparation Guide

Everything you need to know to prepare for and achieve Cyber Essentials Plus certification. From understanding the five technical controls to examination day — this guide walks you through it step by step.

5	8–12	CE+	12mo
TECHNICAL CONTROLS	WEEKS TO PREPARE	HANDS-ON VERIFICATION	CERTIFICATION VALIDITY

1 What is Cyber Essentials Plus?

Cyber Essentials Plus (CE+) is a UK Government-backed cybersecurity certification scheme that provides organisations with a verified level of protection against the most common cyber attacks. Unlike the basic Cyber Essentials certification (which relies on self-assessment), CE+ requires an **independent, hands-on technical audit** conducted by an accredited Certification Body.

The scheme is overseen by the **IASME Consortium** and the **National Cyber Security Centre (NCSC)**. It focuses on five key technical controls that, when properly implemented, can prevent around **80% of cyber attacks**.

Why Does CE+ Matter?

→ **Government contracts:** CE+ is mandatory for many UK Government and MOD contracts involving the handling of sensitive or personal data.

→ **Supply chain trust:** Increasingly required by large enterprises as part of their supplier due diligence process.

→ **Insurance benefits:** Many cyber insurance providers offer reduced premiums for CE+ certified organisations.

→ **Customer confidence:** Demonstrates a verified commitment to cybersecurity — not just a tick-box exercise.

→ **GDPR alignment:** Helps evidence "appropriate technical measures" as required under UK GDPR Article 32.

→ **Competitive advantage:** Differentiates your business from competitors who lack independent verification.

> **CE vs CE+ — Key Difference**
>
> Basic Cyber Essentials is a self-assessed questionnaire. Cyber Essentials Plus adds an independent, hands-on technical verification where an assessor actively tests your systems — scanning for vulnerabilities, testing malware defences, and verifying configurations in person or remotely.

Who Needs CE+?

Any organisation can benefit from CE+, but it is particularly relevant for:

→ **Government suppliers** — required for contracts involving personal or sensitive data

→ **NHS and healthcare providers** — mandated under the Data Security and Protection Toolkit alignment

→ **Defence supply chain** — required under Defence Cyber Protection Partnership (DCPP)

→ **Financial services firms** — expected by regulators and enterprise clients

→ **Any SME handling sensitive data** — demonstrates proportionate security controls

2 The 5 Technical Controls Explained

CE+ is built around five technical controls. Each must be fully implemented and will be independently verified during the assessment.

2.1 Firewalls

Firewalls create a buffer zone between your internal network and external, untrusted networks (e.g., the internet). Every device in scope must be protected by a correctly configured firewall.

- → **Boundary firewalls** must block all inbound connections by default, allowing only explicitly approved services.
- → **Software firewalls** on individual devices must be enabled and configured — especially on laptops used remotely.
- → **Default admin passwords** on firewalls and routers must be changed to strong, unique credentials.
- → Firewall rules must be **documented and reviewed** regularly. Unnecessary open ports must be closed.

2.2 Secure Configuration

Computers and network devices must be configured securely to reduce vulnerabilities. Default settings are often insecure and must be hardened.

- → **Remove or disable unnecessary software**, services, and user accounts from all devices.
- → **Change all default passwords** on all devices, applications, and accounts to unique, strong credentials.
- → **Auto-run/auto-play** must be disabled to prevent malware execution from removable media.
- → Accounts should be configured with the **principle of least privilege** — users only get the access they need.

2.3 Security Update Management

Software vulnerabilities are discovered constantly. Keeping systems up to date is one of the most effective defences against cyber attack.

- → All software in scope must be **licensed and supported** by the vendor (no end-of-life software).
- → **Critical and high-risk patches** must be applied within 14 days of release.
- → This applies to **operating systems, applications, firmware**, and browser plugins.
- → Where automatic updates are available, they should be **enabled by default**.

Common Pitfall: Third-Party Applications

Many organisations keep Windows updated but forget about Adobe Reader, Java, Chrome, Zoom, and other third-party apps. The assessor WILL check these. Use a patch management tool to cover all applications, not just the OS.

2.4 User Access Control

Controlling who has access to your data and services reduces the risk of both accidental and malicious damage.

- → User accounts must be assigned to **named individuals** — no shared or generic accounts.
- → **Admin accounts** must only be used for administrative tasks, never for day-to-day email or browsing.
- → **Standard user accounts** must not have the ability to install software or change system settings.
- → MFA is strongly recommended (and increasingly expected) for **all cloud services and admin access**.

2.5 Malware Protection

Malware (including ransomware, viruses, and spyware) is one of the most common attack vectors. CE+ requires active, verified malware defences.

- → **Anti-malware software** must be installed, active, and set to update automatically on all devices.
- → Software must be configured to **scan files automatically** on access and to perform regular scans.
- → Users must be **prevented from running unapproved applications** via application whitelisting or equivalent controls.
- → The assessor will **test malware defences** during CE+ by attempting to download and execute EICAR test files.

3 Step-by-Step Preparation Checklist

Use this checklist to systematically prepare for each of the five controls before your assessment.

Firewalls Preparation

- □ Audit all internet-facing firewalls and document rulesets
- □ Change default admin passwords on all routers, firewalls, and access points
- □ Verify inbound traffic is blocked by default with only necessary exceptions
- □ Confirm host-based firewalls are enabled on all laptops and desktops
- □ Remove any port-forwarding rules that are no longer needed
- □ Document justification for any open inbound ports

Secure Configuration Preparation

- □ Remove or disable unnecessary software and services from all devices in scope
- □ Change default passwords on all devices, applications, and accounts
- □ Disable auto-run and auto-play on all Windows devices
- □ Confirm user accounts follow the principle of least privilege
- □ Verify screen lock is enabled on all devices (max 15-minute timeout)
- □ Ensure a strong password policy is enforced (min 8 characters, or MFA + min 8)
- □ Disable guest accounts and remove any unused user accounts

Security Update Management Preparation

- □ Verify all operating systems are supported and receiving security updates
- □ Confirm all third-party applications are current (within 14 days for critical patches)
- □ Remove any end-of-life software (e.g., Windows 7, Office 2010, unsupported browsers)
- □ Enable automatic updates where possible across OS and applications
- □ Verify firmware on routers and firewalls is up to date
- □ Document your patch management process and responsible person

User Access Control Preparation

- □ Ensure all user accounts are assigned to named individuals (no shared accounts)
- □ Confirm admin accounts are separate from daily-use accounts
- □ Verify standard users cannot install software or change system settings
- □ Review and remove access for any leavers or inactive accounts
- □ Enable MFA on all cloud services, VPN, and remote access portals

Malware Protection Preparation

- □ Verify anti-malware software is installed and active on all devices in scope
- □ Confirm definitions and signatures update automatically (at least daily)
- □ Ensure real-time scanning is enabled for files on access and web downloads
- □ Test that EICAR test files are blocked on download and execution
- □ Confirm application whitelisting or sandboxing is in place (if not using AV-based approach)

4 Common Pitfalls and How to Avoid Them

These are the most frequent reasons organisations fail their CE+ assessment. Address each one proactively.

PITFALL	WHY IT CAUSES FAILURE	HOW TO AVOID IT
Unpatched third-party software	Assessors scan for ALL known vulnerabilities, not just OS. Outdated Adobe, Java, Chrome, or Zoom will fail.	Use a patch management tool that covers third-party apps. Run a vulnerability scan before your assessment.
End-of-life operating systems	Windows 7, Server 2012, or unsupported macOS versions cannot receive security patches.	Upgrade or decommission all EOL systems before the assessment window.
Users with admin privileges	Standard users who can install software or change settings fail the access control requirement.	Remove local admin rights. Use a separate admin account for IT tasks only.
Default passwords on network devices	Routers, switches, and access points with factory-default credentials are an automatic fail.	Change all default passwords and document the changes.
Missing host firewalls	Personal laptops or desktops without an active software firewall fail even if behind a corporate firewall.	Ensure Windows Firewall or equivalent is enabled and properly configured on every device.
BYOD devices in scope	Personal devices accessing corporate data are in scope and must meet ALL five controls.	Either exclude BYOD from scope or enrol devices in MDM with full compliance enforcement.
Forgotten cloud services	SaaS platforms, cloud email, and web apps are in scope. Misconfigured cloud services are common failures.	Audit all cloud services and ensure MFA, access control, and patching requirements are met.
Malware test failures	The assessor will attempt to download EICAR test files via browser and email. Any successful download fails.	Test EICAR yourself first. Ensure web filtering and endpoint protection block test files at every stage.

Scope Definition Is Critical

One of the biggest mistakes is not clearly defining the scope of your CE+ assessment. EVERY device, user, and service that can access your business data or internet is in scope unless explicitly excluded. This includes home workers' devices, mobile phones, tablets, cloud services, and network equipment. Get scope wrong and you face either an unexpected fail or a much larger assessment than planned.

5 Preparation Timeline: 8–12 Week Plan

Follow this structured timeline to prepare methodically. Adjust timings based on your organisation's size and complexity.

Week 1–2 **Scope & Gap Assessment:** Define your scope boundary. Inventory all devices, users, and services. Conduct an initial gap analysis against the five controls. Identify any end-of-life systems.

Week 3–4 **Firewalls & Network:** Audit and document all firewall rules. Change default passwords on network devices. Close unnecessary ports. Enable host firewalls on all endpoints.

Week 5–6 **Patching & Configuration:** Deploy patch management tooling. Update all OS and third-party software. Remove EOL systems. Harden configurations and disable unnecessary services.

Week 7–8 **Access Control & Malware:** Remove admin rights from standard users. Implement MFA everywhere. Verify anti-malware configuration. Test EICAR file blocking.

Week 9–10 **Internal Testing:** Run your own vulnerability scan. Simulate the assessment process. Verify every device against the checklist. Fix any remaining issues.

Week 11–12 **Assessment Window:** Complete your basic CE self-assessment questionnaire first (required before CE+). Schedule and undergo the CE+ technical assessment with your chosen Certification Body.

6 What to Expect on Examination Day

The CE+ assessment is a hands-on technical verification conducted by an accredited assessor. Here is what happens during the examination.

Before the Assessment

You must first obtain basic **Cyber Essentials certification** (the self-assessment questionnaire). Your CE+ assessment must be conducted within **3 months** of your CE certificate date. The assessor will contact you to confirm scope, schedule the assessment, and explain what access they need.

During the Assessment

The assessment is typically conducted **remotely** (though on-site is possible) and takes between **half a day and two days** depending on the size and complexity of your scope. The assessor will:

- → **External vulnerability scan:** Scan your public-facing IP addresses for known vulnerabilities, open ports, and misconfigurations.
- → **Internal vulnerability scan:** Scan a representative sample of your internal devices (workstations, servers, laptops) for missing patches and vulnerabilities.
- → **Malware protection test:** Attempt to download EICAR test files through web browsers and email on sample devices to verify anti-malware blocks them.
- → **Configuration review:** Check a sample of devices for correct configuration — screen locks, admin rights, password policies, auto-run disabled, firewall status.
- → **Multi-factor authentication check:** Verify MFA is enabled on cloud services and admin accounts by observing a login.
- → **Account privilege review:** Verify standard user accounts cannot install software or change system settings on sample devices.

Sample Size

The assessor does not test every device. They select a **representative sample** based on your scope — typically covering each type of device, operating system, and location. However, if any sampled device fails, they may expand the sample or require remediation across all similar devices.

Assessment Outcomes

Pass

- ✓ Certificate issued, valid for 12 months
- ✓ Listed on the IASME/NCSC register
- ✓ CE+ badge for marketing use
- ✓ Report detailing findings provided

Fail / Remediation Required

- ✗ Assessor provides a detailed report of failures
- ✗ You have a remediation window (typically 30 days)
- ✗ Failed items must be fixed and re-tested
- ✗ Additional fees may apply for re-assessment

Top Tip: Run Your Own Scan First

Before the official assessment, run your own vulnerability scan using tools like Nessus, Qualys, or OpenVAS. This lets you identify and fix issues before the assessor finds them. Focus on missing patches, open ports, and any critical or high-severity vulnerabilities — these will cause an automatic fail.

7 Post-Certification: Maintaining Compliance

Certification is valid for 12 months. Maintaining compliance is an ongoing process, not a one-time project.

Ongoing Requirements

- → **Continuous patching:** Maintain your 14-day critical patch window throughout the year, not just before assessment.
- → **Joiners and leavers:** Ensure new starters are set up with correct access controls, and leavers are disabled promptly.
- → **Device management:** Any new devices entering scope must meet all five controls from day one.
- → **Monthly vulnerability scans:** Run regular internal scans to catch drift or new vulnerabilities early.
- → **Policy reviews:** Review security policies quarterly and update for any changes to scope, technology, or personnel.
- → **Staff awareness:** Continue phishing simulations and security awareness training throughout the year.

Renewal Planning

Start your renewal process **8–10 weeks before** your certificate expires. The renewal process is essentially the same as the initial certification — you must pass a new CE self-assessment followed by a fresh CE+ technical assessment.

TIMEFRAME	ACTION	RESPONSIBLE
10 weeks before expiry	Begin internal gap assessment and pre-scan	IT Manager / Security Lead
8 weeks before expiry	Remediate any findings from pre-scan	IT Team
6 weeks before expiry	Submit CE self-assessment questionnaire	Senior Responsible Officer
4 weeks before expiry	Schedule CE+ assessment with Certification Body	IT Manager
2 weeks before expiry	Final internal checks and readiness confirmation	IT Team
Assessment week	Undergo CE+ technical assessment	All stakeholders

Changes Since Last Certification

The IASME question set and technical requirements are updated periodically. Before renewal, check for any changes to the requirements that may have been introduced since your last certification. Your Certification Body can advise on any new requirements.

Building on CE+

Cyber Essentials Plus is an excellent foundation, but many organisations choose to build further:

→ **ISO 27001:** A comprehensive information security management system (ISMS) that covers governance, risk management, and a wider set of controls.

→ **SOC 2:** Particularly relevant for SaaS providers and US-facing businesses requiring third-party assurance.

→ **NIST Cybersecurity Framework:** A risk-based framework for managing cybersecurity risk across the organisation.

→ **IASME Cyber Assurance:** Extends Cyber Essentials with additional governance, risk management, and incident response requirements.

Quick Reference: The 5 Controls

✓ Firewalls (boundary & host)

✓ Secure Configuration

Key Numbers to Remember

✗ 14-day critical patch window

✗ 12-month certificate validity

Ready to Achieve Cyber Essentials Plus?

Cloudswitched guides organisations through every step — from gap analysis to successful certification.

www.cloudswitched.com/services/cyber-essentials

[redacted]