CLOUDSWITCHED

FREE RESOURCE — PREPARATION GUIDE

Cyber Essentials Plus Preparation Guide

Everything UK SMEs need to prepare for and achieve Cyber Essentials Plus certification — from understanding the five technical controls and avoiding the common failure points to walking through examination day and keeping the certificate alive year-on-year.

5	8–12	80%	12mo
TECHNICAL CONTROLS	WEEKS TO PREPARE	ATTACKS PREVENTED	CERTIFICATE VALIDITY

IASME / NCSC · HANDS-ON AUDIT · UK GOV CONTRACTS · CYBER INSURANCE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Guide & Checklist

01

What is Cyber Essentials Plus?

Cyber Essentials Plus (CE+) is a UK Government-backed cybersecurity certification 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, prevent around **80% of cyber attacks**.

> **CE VS CE+ — THE 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.

Why CE+ matters

- **Government contracts:** mandatory for many UK Government and MOD contracts involving sensitive or personal data.
- **Supply chain trust:** increasingly required by large enterprises as part of supplier due diligence.
- **Insurance benefits:** many cyber insurance providers offer reduced premiums for CE+ certified organisations.
- **GDPR alignment:** helps evidence the "appropriate technical measures" required under UK GDPR Article 32.
- **Competitive advantage:** differentiates your business from competitors with no independent verification.

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 Data Security and Protection Toolkit alignment.
- **Defence supply chain** — required under the Defence Cyber Protection Partnership (DCPP).
- **Financial services firms** — expected by regulators and enterprise clients.

02

The five technical controls

CE+ is built around five technical controls. Each must be fully implemented and will be independently verified during the assessment. This page covers controls 1–3; the next page covers 4–5.

2.1 Firewalls

Firewalls create a buffer zone between your internal network and external, untrusted networks. 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 devices, applications, and accounts to unique, strong credentials.
- **Auto-run and 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**.

02

The five technical controls — continued

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.
- **Multi-factor authentication** 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.

THE EICAR TEST FILE

EICAR is a harmless industry-standard string that every reputable anti-malware product recognises as a virus signature. Assessors use it to verify that your defences block malicious downloads through both browser and email, without putting real malware on your systems. You can test it yourself at **eicar.org** before assessment day.

WHY THE 5 CONTROLS WORK

The NCSC's evidence shows that these five controls — firewalls, secure configuration, patching, access control, and malware protection — collectively prevent **around 80% of common cyber attacks**. They are deliberately the minimum baseline a competent organisation should run, not a ceiling.

03

Step-by-step preparation checklist

Use this checklist to systematically prepare for each of the five controls before your assessment. Tick every item that is **fully in place** — not partial, not "we're working on it". This is an **interactive PDF** — you can tick the boxes directly in any modern PDF viewer.

2.1 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.

2.2 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 *(maximum 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.

03

Step-by-step preparation checklist — continued

2.3 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 the responsible person.

2.4 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.

2.5 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 relying on AV alone.

04

Common pitfalls and how to avoid them

These are the most frequent reasons organisations fail their CE+ assessment. Address each one proactively well before assessment day — a clean run starts with knowing where most failures come from.

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 opens.
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 for the assessor.
Missing host firewalls	Laptops or desktops without an active software firewall fail even when behind a corporate firewall.	Ensure Windows Firewall or equivalent is enabled and properly configured on every device.
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. A 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 — that 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.

05

Preparation timeline: 8–12 week plan

Follow this structured timeline to prepare methodically. Adjust timings based on your organisation's size and complexity — a 5-person firm with everything in Microsoft 365 will move faster than a 60-person firm with mixed on-premise and cloud.

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 and 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 every endpoint.
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 on browser and email.
WEEK 9-10	**Internal testing:** run your own vulnerability scan. Simulate the assessment process. Verify every device against the checklist. Fix any remaining issues before the assessor arrives.
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.

THE CE FIRST, CE+ SECOND RULE

You must hold a current basic Cyber Essentials certificate **before** you can sit the CE+ assessment, and the CE+ audit must be completed **within 3 months** of your CE certificate date. Plan the two together — do not let the CE certificate expire mid-prep.

06

What to expect on examination day

The CE+ assessment is a hands-on technical verification conducted by an accredited assessor. Here is what happens before, during, and after the examination so nothing on the day comes as a surprise.

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 internal devices — workstations, servers, laptops — for missing patches.
- **Malware protection test:** attempt to download EICAR test files through web browsers and email on sample devices to verify the 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.

Assessment outcomes

PASS

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

FAIL — REMEDIATION REQUIRED

- Detailed report of failures from the assessor
- Remediation window (typically 30 days)
- Failed items must be fixed and re-tested
- Additional fees may apply for re-assessment

07

Post-certification — maintaining compliance

Certification is valid for 12 months. Maintaining compliance is an ongoing process, not a one-time project. Treat the certificate as the visible outcome of a year-round discipline, not as a once-a-year sprint.

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 (target: within 24 hours).
- **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. Renewal is essentially the same as initial certification — pass a new CE self-assessment, then sit 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

08

Building on CE+ & quick reference

Cyber Essentials Plus is an excellent foundation, but many organisations choose to build further as their risk profile or client base grows. Below: the most common next steps, plus a one-page reminder of everything in this guide.

Beyond CE+ — the natural next steps

ISO 27001: a comprehensive information security management system (ISMS) covering governance, risk management, and a wider control set.

SOC 2: particularly relevant for SaaS providers and US-facing businesses requiring third-party assurance reports for enterprise customers.

NIST Cybersecurity Framework: a risk-based framework for managing cybersecurity risk across the organisation, useful when CE+ alone no longer maps cleanly to your exposure.

IASME Cyber Assurance: extends Cyber Essentials with additional governance, risk management, and incident response requirements — the natural sister track to CE+.

Quick reference

THE 5 CONTROLS

- Firewalls (boundary & host)
- Secure Configuration
- Security Update Management
- User Access Control
- Malware Protection

KEY NUMBERS TO REMEMBER

- 14-day critical patch window
- 12-month certificate validity
- 3-month CE to CE+ window
- 8–12 weeks preparation time
- 80% of attacks prevented

CLOUDSWITCHED

CYBER SECURITY & COMPLIANCE FOR UK SMES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom