Cyber Essentials Plus Requirements Checklist

A comprehensive checkbox checklist covering every requirement across the five CE+ control areas. Use this to track readiness, gather evidence, and confirm pass/fail criteria before your assessment.

5	40+	☐	P/F
CONTROL AREAS	INDIVIDUAL REQUIREMENTS	TRACK YOUR READINESS	PASS / FAIL CRITERIA

How to Use This Checklist

Work through each control area systematically. For every requirement, tick the checkbox when fully in place, note the evidence you have, and confirm whether it meets the pass/fail criteria. All items must pass for successful CE+ certification. Use the scoring section at the end to track overall readiness.

1 Control 1: Firewalls

Firewalls protect your network boundary and individual devices from unauthorised access.

☐	REQUIREMENT	EVIDENCE NEEDED	PASS / FAIL CRITERIA
☐	**Boundary firewall** is installed between internal network and the internet	Firewall model, configuration screenshots, rule export	A hardware or software firewall must exist at every internet boundary
☐	**Default admin password** on firewall/router has been changed	Evidence that default credentials no longer work	Default passwords must not be in use on any network device
☐	**Inbound firewall rules** block all traffic by default, with only documented exceptions	Firewall rule export showing deny-all inbound default	No unnecessary inbound ports open; each exception documented
☐	Approved inbound rules have documented **business justification**	Written justification for each allow rule	Every open port must have a named business reason
☐	Unapproved services are **blocked or not running**	Port scan results showing no unexpected services	External scan reveals no unapproved listening services
☐	**Host-based firewall** is enabled on every device (especially laptops)	Device configuration screenshots or MDM compliance report	Windows Firewall or equivalent must be ON for all profiles
☐	Host firewall **blocks inbound connections** by default on untrusted networks	Firewall profile settings for Public/Guest networks	Must block inbound when on public/untrusted networks
☐	**Administrative interfaces** are not accessible from the internet (or protected by MFA)	Port scan and access test results	No admin consoles reachable externally without strong controls

Control 1 — Firewalls: ____/8 items

2 Control 2: Secure Configuration

Devices and software must be configured to reduce vulnerabilities and remove unnecessary functionality.

	REQUIREMENT	EVIDENCE NEEDED	PASS / FAIL CRITERIA
☐	**Unnecessary software** has been removed or disabled from all devices	Software inventory showing only approved applications	No bloatware, trial software, or unused services running
☐	**Default user accounts** (Guest, Admin) are disabled or have changed passwords	Account list showing disabled defaults	No device uses default or generic credentials
☐	**Password policy** enforces minimum 8 characters (or 8+ with MFA)	GPO settings, Entra ID policy screenshots	Password complexity requirements met across all systems
☐	**Account lockout** or throttling is configured (max 10 failed attempts)	Lockout policy configuration	Accounts lock or throttle after no more than 10 failed attempts
☐	**Auto-run/auto-play** is disabled on all Windows devices	Registry or GPO settings	Inserting USB media must not auto-execute content
☐	**Screen lock** activates after a maximum of 15 minutes of inactivity	GPO or MDM policy showing timeout setting	All devices must lock screen within 15 minutes max
☐	A **known and approved build/configuration** standard exists for each device type	SOE documentation or build checklist	Consistent, documented build standard across device types
☐	**Unnecessary network services** are disabled (Telnet, FTP, etc.)	Service audit results	No insecure or unnecessary services running on any device

Control 2 — Secure Configuration: ____ /8 items

3 Control 3: Security Update Management

All software must be kept up to date to protect against known vulnerabilities.

	REQUIREMENT	EVIDENCE NEEDED	PASS / FAIL CRITERIA
☐	All **operating systems** are supported and receiving vendor security updates	OS version inventory across all devices	No end-of-life OS (e.g., Windows 7, Server 2012, unsupported macOS)
☐	All **applications** are licensed, supported, and receiving updates	Application inventory with version numbers	No end-of-life or unsupported applications in scope
☐	**Critical/high-risk patches** are applied within 14 days of release	Patch compliance report showing deployment dates	Vulnerability scan shows no critical patches older than 14 days
☐	**All other patches** are applied in a reasonable timeframe	Patch management reports	Medium/low patches applied regularly; no excessive backlog
☐	**Automatic updates** are enabled where available	Update settings screenshots or policy configuration	Auto-update enabled for OS and major applications
☐	**Third-party software** (Adobe, Chrome, Java, Zoom) is patched to current versions	Third-party patch report or vulnerability scan	No known high/critical vulnerabilities in third-party apps
☐	**Firmware** on routers, firewalls, and network devices is up to date	Firmware version check against vendor latest	Network device firmware within supported versions
☐	**Browser plugins** and extensions are current and approved	Browser extension audit	No outdated or unapproved browser plugins

Control 3 — Security Updates: ____ /8 items

4 Control 4: User Access Control

Access to data and services must be controlled to minimise the risk of unauthorised access or misuse.

	REQUIREMENT	EVIDENCE NEEDED	PASS / FAIL CRITERIA
☐	All accounts are assigned to **named individuals** (no shared/generic accounts)	User account list showing named individuals	Every active account maps to a specific person
☐	**Admin accounts** are separate from standard user accounts	Account audit showing separate admin accounts	Admin tasks use dedicated admin accounts, not daily-use accounts
☐	**Standard users cannot install** software or change system settings	UAC settings, GPO, or MDM policy evidence	Login as standard user and confirm inability to install .exe
☐	**Admin accounts are not used** for email, web browsing, or daily tasks	Login audit showing admin account usage patterns	Admin accounts restricted to administrative activities only
☐	**MFA is enabled** on all cloud services and remote access	MFA configuration screenshots, Conditional Access policies	MFA prompt observed when logging in to cloud services
☐	**Leavers/role changes** process removes or adjusts access promptly	Documented process and recent examples	Access removed within 24 hours of leaving
☐	**User access reviews** are conducted regularly	Access review records from the past 12 months	Evidence of periodic review and removal of unnecessary access
☐	**Unique credentials** are required for each user on each service	No evidence of credential sharing or group passwords	Each user has unique username and password per service

Control 4 — User Access Control: ____/8 items

5 Control 5: Malware Protection

Active malware defences must be in place to prevent, detect, and respond to malicious software.

	REQUIREMENT	EVIDENCE NEEDED	PASS / FAIL CRITERIA
☐	**Anti-malware software** is installed and active on all in-scope devices	Endpoint protection dashboard showing all devices	Every in-scope device has active AV/EDR with current status
☐	Malware signatures/definitions **update automatically** (minimum daily)	Update log or configuration showing auto-update	Definitions no older than 1 day on any device
☐	**Real-time/on-access scanning** is enabled	AV configuration screenshots	Files scanned automatically when opened or downloaded
☐	**Web browsing protection** blocks access to known malicious websites	Web filtering or DNS protection configuration	Attempting to visit known malicious URL is blocked
☐	**EICAR test file** is blocked on download via web browser	Test result showing EICAR blocked	Assessor downloads EICAR — must be blocked or quarantined
☐	**EICAR test file** is blocked on download via email attachment	Test result showing EICAR blocked in email	EICAR attachment must be blocked before reaching user inbox
☐	**Application whitelisting** or sandboxing prevents unapproved code execution	AppLocker, WDAC, or equivalent configuration	Users cannot run executables from unapproved locations
☐	Anti-malware **cannot be disabled** by standard users	Configuration showing tamper protection enabled	Standard user attempt to disable AV is blocked

Control 5 — Malware Protection: ____/8 items

Important: All Controls Must Pass

Unlike some certifications with partial compliance, CE+ is a **pass/fail assessment**. Every requirement in every control area must be met. A single failed item in any control area can result in overall failure. If remediation is required, the assessor will specify a window (usually 30 days) for you to fix issues and be re-tested.

★ Evidence Gathering Guide

For each control area, you need to be ready to provide evidence to the assessor. This table summarises the typical evidence types.

CONTROL AREA	TYPICAL EVIDENCE	FORMAT	WHEN NEEDED
Firewalls	Firewall configuration exports, rule documentation, port scan results	PDF / CSV export	Before & during assessment
Secure Configuration	GPO settings, build standard document, software inventory	Screenshots / docs	During assessment
Security Updates	Patch compliance reports, vulnerability scan results, OS inventory	Scan reports	Within 7 days of assessment
User Access Control	User account lists, MFA configuration, access review records	Screenshots / logs	During assessment
Malware Protection	AV dashboard, EICAR test results, web filter configuration	Screenshots / live demo	Live during assessment

Tip: Prepare an Evidence Folder

Create a dedicated folder with sub-folders for each control area. Collect screenshots, configuration exports, and reports as you prepare. Having organised evidence ready on assessment day speeds up the process significantly and demonstrates a mature approach to security management.

★ Scope Confirmation Checklist

Before your assessment, confirm the scope of your CE+ certification. Every item in scope must meet ALL five controls.

Devices in Scope

- [ ] **Desktop computers** — all company-owned desktops used for business
- [ ] **Laptops** — all company-owned laptops including those used at home
- [ ] **Servers** — all on-premise and cloud-hosted servers (including virtual)
- [ ] **Mobile devices** — any phones or tablets accessing business email or data
- [ ] **BYOD devices** — personal devices accessing any corporate resource
- [ ] **Network equipment** — routers, switches, access points, firewalls
- [ ] **Cloud services** — Microsoft 365, Google Workspace, AWS, Azure, SaaS apps
- [ ] **Thin clients / VDI** — any devices connecting to virtual desktop infrastructure

Services in Scope

- [ ] **Email service** (Microsoft 365, Google Workspace, etc.)
- [ ] **File storage** (OneDrive, SharePoint, Google Drive, network shares)
- [ ] **CRM / ERP** systems (Salesforce, HubSpot, Xero, etc.)
- [ ] **VPN / remote access** solutions
- [ ] **Website hosting** and any web applications you manage
- [ ] **Backup services** (cloud backup, on-premise backup servers)

★ Overall Readiness Scoring

Use this scoring summary to track your readiness across all five control areas. Complete all items before scheduling your assessment.

#	CONTROL AREA	ITEMS READY	ITEMS REMAINING	STATUS
1	Firewalls	/ 8		Ready / Not Ready
2	Secure Configuration	/ 8		Ready / Not Ready
3	Security Update Management	/ 8		Ready / Not Ready
4	User Access Control	/ 8		Ready / Not Ready
5	Malware Protection	/ 8		Ready / Not Ready
TOTAL READINESS		**/ 40**		**Assessment Ready: Yes / No**

Readiness Interpretation

40/40 items ready: You are ready to schedule your CE+ assessment. Ensure evidence is organised and accessible.
30–39 items ready: Close but gaps remain. Address all outstanding items before booking — any single failure can block certification.
Below 30 items: Significant preparation still needed. Focus on the highest-risk gaps and consider engaging specialist support.

Assessment Sign-Off

Prepared by: .....

Date completed: .....

Assessment booked for: .....

Certification Body: .....

Approved by: .....