CLOUDSWITCHED

FREE RESOURCE — CE+ CHECKLIST

Cyber Essentials Plus Requirements

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	Fillable
CONTROL AREAS IN SCOPE	INDIVIDUAL REQUIREMENTS	ALL CONTROLS MUST PASS	TICK & TYPE IN ANY VIEWER

FIREWALLS · SECURE CONFIG · PATCHING · ACCESS CONTROL · MALWARE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through each of the five CE+ control areas with your IT team or MSP. Tick every requirement that is **fully in place** — in production and verifiable today, not partially, not "we're working on it". Record the evidence you can produce on assessment day, and confirm the pass/fail criterion is met.

CE+ IS PASS/FAIL

A single failed item in any control area fails the whole certification. Use this checklist before booking so you walk in knowing every requirement is met — not finding out under audit pressure. Tick only when there is evidence: a configuration export, a screenshot, a policy, a test result.

The five control areas

- **01 Firewalls** — boundary and host firewalls, default credentials, inbound rules, admin interfaces.
- **02 Secure Configuration** — build standards, default accounts, password policy, auto-run, screen lock.
- **03 Security Update Management** — supported OS, patch SLAs, auto-update, third-party, firmware.
- **04 User Access Control** — named accounts, admin separation, MFA, leavers, access reviews.
- **05 Malware Protection** — EDR/AV, real-time scanning, web and email filtering, EICAR tests.

CE FIRST, THEN CE+

You must pass the basic Cyber Essentials self-assessment **before** the CE+ technical assessment. The CE+ assessment must occur within 3 months of your CE certificate date — plan both together to avoid timing issues.

01

Control 1 — Firewalls

Firewalls protect your network boundary and individual devices from unauthorised access. The assessor will verify both boundary and host firewall configurations and test that admin interfaces are not reachable from the internet.

- ☐ **Boundary firewall** is installed between the internal network and the internet.
  EVIDENCE Firewall model, configuration screenshots, rule export.
  PASS/FAIL A hardware or software firewall must exist at every internet boundary.

- ☐ **Default admin password** on every firewall and router has been changed.
  EVIDENCE Test showing default credentials no longer work.
  PASS/FAIL Default passwords must not be in use on any network device.

- ☐ **Inbound firewall rules** block all traffic by default, with only documented exceptions.
  EVIDENCE Rule export showing deny-all inbound default.
  PASS/FAIL No unnecessary inbound ports open; each exception documented.

- ☐ Each approved inbound rule has a documented **business justification**.
  EVIDENCE Written justification for every allow rule.
  PASS/FAIL Every open port must have a named business reason.

- ☐ Unapproved services are **blocked or not running**.
  EVIDENCE External port scan results.
  PASS/FAIL External scan reveals no unapproved listening services.

- ☐ **Host-based firewall** is enabled on every device, especially laptops.
  EVIDENCE Device or MDM compliance screenshots.
  PASS/FAIL Windows Firewall (or equivalent) ON for all profiles.

- ☐ Host firewall **blocks inbound connections** by default on untrusted networks.
  EVIDENCE Public/Guest profile settings.
  PASS/FAIL Must block inbound on public/untrusted networks.

- ☐ **Administrative interfaces** are not reachable from the internet, or are protected by MFA.
  EVIDENCE Port scan and access-test results.
  PASS/FAIL No admin consoles reachable externally without strong controls.

EVIDENCE COLLECTED _____ **OWNER** _____

REVIEW DATE _____ **NOTES** _____

CONTROL 1 ITEMS PASSED _____ / **8** *All 8 must pass for CE+ certification.*

02

Control 2 — Secure Configuration

Devices and software must be configured to reduce vulnerabilities and remove unnecessary functionality. The assessor will sample devices to confirm builds, default accounts and password policy match a documented standard.

- ☐ **Unnecessary software** has been removed or disabled on all devices.
  EVIDENCE Software inventory of approved applications only. **PASS/FAIL** No bloatware, trial software or unused services running.

- ☐ **Default user accounts** (Guest, Admin) are disabled or have changed passwords.
  EVIDENCE Account list showing disabled defaults. **PASS/FAIL** No device uses default or generic credentials.

- ☐ **Password policy** enforces minimum 8 characters (or 8+ with MFA).
  EVIDENCE GPO settings, Entra ID policy screenshots. **PASS/FAIL** Complexity requirements met across all systems.

- ☐ **Account lockout** or throttling is configured (max 10 failed attempts).
  EVIDENCE Lockout policy configuration screenshot. **PASS/FAIL** Accounts lock or throttle after no more than 10 failed attempts.

- ☐ **Auto-run/auto-play** is disabled on all Windows devices.
  EVIDENCE Registry or GPO settings. **PASS/FAIL** USB media must not auto-execute content.

- ☐ **Screen lock** activates after no more than 15 minutes of inactivity.
  EVIDENCE GPO or MDM policy with timeout setting. **PASS/FAIL** All devices must lock within 15 minutes max.

- ☐ A known and approved **build/configuration standard** exists for each device type.
  EVIDENCE SOE document or build checklist. **PASS/FAIL** Consistent, documented build standard per device type.

- ☐ **Unnecessary network services** are disabled (Telnet, FTP, etc.).
  EVIDENCE Service audit results. **PASS/FAIL** No insecure or unnecessary services running on any device.

EVIDENCE COLLECTED	OWNER
REVIEW DATE	**NOTES**

CONTROL 2 ITEMS PASSED _____ / **8** *All 8 must pass for CE+ certification.*

03

Control 3 — Security Update Management

All software must be kept up to date to protect against known vulnerabilities. The assessor will run a vulnerability scan; any critical or high patch older than 14 days fails this control.

- ☐ All **operating systems** are supported and receiving vendor security updates.
  EVIDENCE OS version inventory across all devices. **PASS/FAIL** No end-of-life OS (Win 7, Server 2012, unsupported macOS).

- ☐ All **applications** are licensed, supported and receiving updates.
  EVIDENCE Application inventory with version numbers. **PASS/FAIL** No end-of-life or unsupported applications in scope.

- ☐ **Critical/high-risk patches** are applied within 14 days of release.
  EVIDENCE Patch compliance report with deployment dates. **PASS/FAIL** Vuln scan shows no critical patches older than 14 days.

- ☐ **All other patches** are applied within a reasonable timeframe.
  EVIDENCE Patch management reports. **PASS/FAIL** Medium/low patches applied regularly; no excessive backlog.

- ☐ **Automatic updates** are enabled where available.
  EVIDENCE Update settings screenshots or policy configuration. **PASS/FAIL** Auto-update enabled for OS and major applications.

- ☐ **Third-party software** (Adobe, Chrome, Java, Zoom) is on current versions.
  EVIDENCE Third-party patch report or vulnerability scan. **PASS/FAIL** No known high/critical vulnerabilities in third-party apps.

- ☐ **Firmware** on routers, firewalls and network devices is up to date.
  EVIDENCE Firmware version check against vendor latest. **PASS/FAIL** Network device firmware within supported versions.

- ☐ **Browser plugins** and extensions are current and approved.
  EVIDENCE Browser extension audit. **PASS/FAIL** No outdated or unapproved browser plugins.

EVIDENCE COLLECTED _____ **OWNER** _____

REVIEW DATE _____ **NOTES** _____

CONTROL 3 ITEMS PASSED _____ / **8** *All 8 must pass for CE+ certification.*

04

Control 4 — User Access Control

Access to data and services must be controlled to minimise the risk of unauthorised access or misuse. The assessor will sample accounts to confirm separation of admin from daily-use, MFA enforcement and a working leaver process.

- ☐ All accounts are assigned to **named individuals**; no shared or generic accounts.
  EVIDENCE User account list showing named individuals. **PASS/FAIL** Every active account maps to a specific person.

- ☐ **Admin accounts** are separate from standard user accounts.
  EVIDENCE Account audit showing separate admin accounts. **PASS/FAIL** Admin tasks use dedicated admin accounts.

- ☐ **Standard users cannot install** software or change system settings.
  EVIDENCE UAC, GPO or MDM policy evidence. **PASS/FAIL** Login as standard user; install of .exe must be blocked.

- ☐ **Admin accounts are not used** for email, web browsing or daily tasks.
  EVIDENCE Login audit of admin account usage patterns. **PASS/FAIL** Admin accounts restricted to administrative activity only.

- ☐ **MFA is enabled** on all cloud services and remote access.
  EVIDENCE MFA config screenshots, Conditional Access policies. **PASS/FAIL** MFA prompt observed when logging in to cloud services.

- ☐ **Leavers and role changes** process removes or adjusts access promptly.
  EVIDENCE Documented process and recent examples. **PASS/FAIL** Access removed within 24 hours of leaving.

- ☐ **User access reviews** are conducted regularly.
  EVIDENCE Access review records from the past 12 months. **PASS/FAIL** Evidence of periodic review and access removal.

- ☐ **Unique credentials** are required for each user on each service.
  EVIDENCE No evidence of credential sharing or group passwords. **PASS/FAIL** Each user has unique username and password per service.

EVIDENCE COLLECTED _____ **OWNER** _____

REVIEW DATE _____ **NOTES** _____

CONTROL 4 ITEMS PASSED _____ / **8** *All 8 must pass for CE+ certification.*

05

Control 5 — Malware Protection

Active malware defences must be in place to prevent, detect and respond to malicious software. The assessor will run live EICAR tests via both web download and email attachment — both must be blocked before reaching the user.

- ☐ **Anti-malware software** is installed and active on all in-scope devices.
  EVIDENCE Endpoint protection dashboard. **PASS/FAIL** Every in-scope device has active AV/EDR with current status.

- ☐ Malware signatures/definitions **update automatically** (minimum daily).
  EVIDENCE Update log or config showing auto-update. **PASS/FAIL** Definitions no older than 1 day on any device.

- ☐ **Real-time/on-access scanning** is enabled.
  EVIDENCE AV configuration screenshots. **PASS/FAIL** Files scanned automatically when opened or downloaded.

- ☐ **Web browsing protection** blocks known malicious websites.
  EVIDENCE Web filtering or DNS protection configuration. **PASS/FAIL** Attempting to visit known malicious URL is blocked.

- ☐ **EICAR test file** is blocked on download via web browser.
  EVIDENCE Test result showing EICAR blocked. **PASS/FAIL** Assessor downloads EICAR — must be blocked or quarantined.

- ☐ **EICAR test file** is blocked when delivered as an email attachment.
  EVIDENCE Test result showing EICAR blocked in email. **PASS/FAIL** Attachment must be blocked before reaching the user inbox.

- ☐ **Application whitelisting** or sandboxing prevents unapproved code execution.
  EVIDENCE AppLocker, WDAC or equivalent configuration. **PASS/FAIL** Users cannot run executables from unapproved locations.

- ☐ Anti-malware **cannot be disabled** by standard users.
  EVIDENCE Configuration showing tamper protection enabled. **PASS/FAIL** Standard user attempt to disable AV is blocked.

EVIDENCE COLLECTED _____ **OWNER** _____

REVIEW DATE _____ **NOTES** _____

CONTROL 5 ITEMS PASSED _____ / **8** *All 8 must pass for CE+ certification.*

06

Evidence gathering guide

For each control area you must be ready to produce specific evidence when the assessor asks. Collect the items in this table into a single evidence folder organised by control number, and have it on the screen at assessment start.

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

PREPARE AN EVIDENCE FOLDER

Create a dedicated folder with sub-folders *01-Firewalls*, *02-Secure-Config*, *03-Patching*, *04-Access*, *05-Malware*. Collect screenshots, configuration exports and reports as you work through this checklist. Having organised, dated evidence ready on assessment day speeds up the process and signals a mature security posture to the assessor.

ALL CONTROLS MUST PASS

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 (typically 30 days) for you to fix issues and be re-tested.

EVIDENCE FOLDER LOCATION

OWNER

LAST REFRESHED

NOTES

07

Scope confirmation checklist

Before your assessment, confirm the scope of your CE+ certification. Every item in scope must meet ALL five controls. Anything in scope but failing a single control fails the whole certification — so be honest about scope rather than discovering gaps under audit.

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 (incl. virtual).
- ☐ **Mobile devices** — 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** — M365, Google Workspace, AWS, Azure, SaaS apps.
- ☐ **Thin clients / VDI** — any devices connecting to virtual desktops.

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).

SCOPE CONFIRMED BY _____

OWNER _____

REVIEW DATE _____

NOTES _____

Σ

Overall readiness scoring

Transfer the score for each control area into the table. Tick the readiness status box once every requirement in that control is in production with evidence. Anything not at **Ready** blocks certification.

#	CONTROL AREA	ITEMS READY	REMAINING	STATUS
01	**Firewalls**	_____ / 8	_____	☐ R ☐ P ☐ N
02	**Secure Configuration**	_____ / 8	_____	☐ R ☐ P ☐ N
03	**Security Update Management**	_____ / 8	_____	☐ R ☐ P ☐ N
04	**User Access Control**	_____ / 8	_____	☐ R ☐ P ☐ N
05	**Malware Protection**	_____ / 8	_____	☐ R ☐ P ☐ N
Σ	**TOTAL READINESS**	_____ / **40**	_____	☐ **R** ☐ **P** ☐ **N**

Readiness interpretation

`40 / 40`	**Ready.** All controls passed. Book your CE+ technical assessment and have the evidence pack accessible on assessment day.
`30 - 39`	**Close, but gaps remain.** Address every outstanding item before booking — any single failure blocks certification.
`Below 30`	**Significant preparation needed.** Focus on the highest-risk gaps and engage specialist support to close them before assessment.

REMEMBER: CE SELF-ASSESSMENT FIRST

You must pass the basic Cyber Essentials self-assessment questionnaire **before** your CE+ technical assessment can take place. The CE+ assessment must occur within 3 months of your CE certificate date. Plan both assessments together to avoid timing issues.

Assessment sign-off & next steps

Once every control area is ready, capture sign-off here and book the technical assessment. The signatures and dates below form part of your internal evidence pack — they show governance was in place before the assessor arrived.

Top three remediation priorities

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

Sign-off

PREPARED BY _____

DATE COMPLETED _____

ASSESSMENT BOOKED FOR _____

CERTIFICATION BODY _____

APPROVED BY _____

SIGNATURE _____

Need help preparing for CE+ certification?

Cloudswitched provides end-to-end support — gap analysis, remediation, evidence packs and the live assessment — with fixed-price quotes and a track record of first-time passes.

info@cloudswitched.com

cloudswitched.com/services/cyber-essentials

CLOUDSWITCHED

CYBER SECURITY & COMPLIANCE

info@cloudswitched.com

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