SURECLOUD®

GRC READINESS TOOLKIT

EXECUTABLE GRC

Cyber Essentials Certification Checklist.

Everything you need in place before you open the questionnaire. Scope, the five controls, ASP selection, submission, and renewal — in one working checklist.

- Scope
- The five controls
- ASP selection
- Submission
- Renewal & CE+

Aligned to the **IASME Montpellier** scheme requirements current as of 2026.
Companion to the SureCloud Cyber Essentials Checklist guide.

BEFORE YOU START

Six things that decide the outcome.

Most failed assessments come down to a handful of avoidable mistakes. Get these right before you open the questionnaire and the rest of the process is largely administrative.

01 · SCOPE FIRST

Define your boundary before you start.

Decide which devices, users, and cloud services fall within scope first. **Wrong scope is the most common cause of unexpected remediation.**

02 · ASP ROUTE

You can't submit directly to IASME.

Certification goes through an **Assured Service Provider** via the Montpellier portal. Choose yours before you start.

03 · PATCHING

14 days, no exceptions.

Patch management is the most common failure point. Critical and high-severity patches must be applied within 14 days. **End-of-life software is an automatic failure.**

04 · MFA

Mandatory on internet-facing accounts.

MFA is required on all accounts that can authenticate to internet-facing services — a **Montpellier scheme requirement introduced in 2023.**

05 · VALIDITY

Certificates last 12 months.

Requirements can change between cycles, so **check for updates before resubmitting** rather than re-using last year's answers.

06 · CE+ WINDOW

Three months, then it lapses.

Initiate CE+ within three months of standard CE certification, or you **restart the standard CE process.**

Your certification path

1. **Scope your certification** — Define the systems, users, and services in scope.
2. **Meet the five controls** — Firewalls, configuration, access, malware, patching.
3. **Select an ASP** — Choose an IASME-approved Assured Service Provider.
4. **Submit the questionnaire** — Self-assess via the Montpellier portal.
5. **Plan annual renewal** — Re-certify every 12 months against current rules.
6. **CE+ track (optional)** — Add independent technical verification.

1 STEP ONE

Scope your certification.

The scope defines which systems, devices, and users are covered. Everything in scope must meet all five control requirements. Agree it with your ASP **before** you open the questionnaire.

- [ ] Document all devices that can access internet-facing services: laptops, desktops, servers, mobile devices, and virtual machines.
- [ ] Identify all cloud services where your organisation controls configuration (Microsoft 365, AWS, Azure, Google Workspace tenancies).
- [ ] Identify any devices or services explicitly excluded from scope and document the rationale, in line with IASME exclusion guidance.
- [ ] Confirm your scope boundary covers the full set of systems involved in your organisation's core operations.
- [ ] Review IASME scope guidance for BYOD and home-working devices. Devices used to access work systems from outside the office may be in scope.

SCOPE SETS EVERYTHING DOWNSTREAM

Scope errors cascade. A device or cloud tenancy you forget to include can surface during ASP review as a control gap — and trigger remediation late, when it costs the most. Treat the scope declaration as the foundation of the whole assessment, not a formality.

The five controls you're scoping for

1	**Firewalls**	Boundary and personal firewalls protecting your networks and devices.
2	**Secure configuration**	Devices and software hardened to reduce attack surface.
3	**User access control**	Least-privilege access with administrative privileges protected.
4	**Malware protection**	Anti-malware or application allowlisting across in-scope devices.
5	**Patch management**	All software kept current — the most common cause of failure.

2

STEP TWO

The five control areas.

5/5 All five controls must be met across **all in-scope systems**. Partial compliance does not achieve certification. Items below reflect Montpellier scheme requirements current as of 2026.

1 Firewalls

A firewall at the boundary between your network and the internet, plus personal firewalls on devices used outside a protected network.

- [ ] A firewall (hardware or software) is configured at the network boundary.
- [ ] All unused and unnecessary inbound network ports are blocked by default.
- [ ] Firewall rules are documented and reviewed. Rules are specific, not permissive.
- [ ] Personal firewalls are enabled on all laptops, desktops, and mobile devices used outside the office network, including home-working devices.
- [ ] Administrative access to firewall management interfaces is restricted to authorised users and, where possible, specific IP addresses.
- [ ] Default administrative credentials on all firewalls and network devices have been changed.

2 Secure configuration

In-scope devices and software configured to reduce attack surface: remove unnecessary features, disable unused services, eliminate insecure defaults.

- [ ] Default passwords on all hardware and software have been changed before devices are deployed.
- [ ] Unnecessary user accounts, including default vendor accounts, have been disabled or removed.
- [ ] Unnecessary software, services, and features have been uninstalled or disabled on in-scope devices.
- [ ] Auto-run features (USB, CD, network shares) are disabled.
- [ ] Devices lock automatically after a period of inactivity, requiring re-authentication to resume.
- [ ] All in-scope systems use supported operating systems and software that still receive vendor security updates.

3 User access control

Access limited to what each role requires. Administrative privileges controlled and protected.

- [ ] User accounts are created on a least-privilege basis: users have only the permissions their role requires.
- [ ] Administrative accounts are separate from standard user accounts. Staff don't use admin accounts for day-to-day tasks.
- [ ] The number of administrator accounts is minimised and reviewed regularly.
- [ ] MFA is enforced on all accounts that can authenticate to internet-facing services, including cloud applications, email, and remote access. MONTPELLIER 2023
- [ ] Passwords meet minimum complexity requirements, or MFA is used as the primary authentication mechanism.
- [ ] Guest or shared accounts that serve no current purpose have been removed.
- [ ] A process exists to promptly remove or disable accounts when staff leave or change roles.

4 Malware protection

In-scope devices protected against malware, either through anti-malware software or application allowlisting.

- [ ] Anti-malware software is installed and active on all in-scope devices, or application allowlisting is configured to prevent unauthorised software from executing.
- [ ] Anti-malware software is configured to update its definitions automatically.
- [ ] Anti-malware scans are scheduled or run in real time.
- [ ] Anti-malware alerts on detection and is monitored. Detections are reviewed, not ignored.
- [ ] If using allowlisting: only approved applications can execute, and the allowlist is actively maintained and reviewed.

5 Patch management

The control most commonly responsible for assessment failures. All software on in-scope devices kept up to date.

- [ ] All operating systems on in-scope devices receive automatic security updates, or a process applies critical and high-severity patches **within 14 days** of release.
- [ ] All third-party applications are kept up to date: browsers, productivity software, plugins, and any other installed applications.
- [ ] A software inventory exists for all in-scope devices. You know what's installed and whether it's currently supported.
- [ ] Any end-of-life software has been removed or replaced. AUTOMATIC FAILURE
- [ ] A process is in place to monitor vendor announcements for critical vulnerabilities and respond within the 14-day window.

STEP THREE

3 Select an Assured Service Provider.

CE assessments must be conducted through an IASME-approved ASP, which reviews and certifies your submission. For CE+, the ASP must also have qualified assessors for technical verification.

- [ ] Search the IASME-published ASP directory for accredited providers.
- [ ] Confirm the ASP is accredited for CE, and for CE+ if applicable.
- [ ] Confirm pricing and what's included. Some bundle pre-assessment support; others don't.
- [ ] Confirm whether the assessment uses the Montpellier portal or a separate ASP-managed system. Most use the IASME Montpellier portal.

4

STEP FOUR

Complete and submit the questionnaire.

The self-assessment is completed via the IASME Montpellier portal, attesting to compliance with each of the five controls across all in-scope systems.

- [ ] Create or log in to your Montpellier portal account, via your ASP or directly through IASME.
- [ ] Complete the scope declaration: describe the systems and boundary covered by the assessment.
- [ ] Work through each of the five control sections, answering accurately based on your actual configuration.
- [ ] Review your answers for internal consistency before submission. The ASP review checks for contradictions.
- [ ] Submit the completed questionnaire through the portal.
- [ ] Respond promptly to ASP clarification requests. Delayed responses extend the assessment timeline.

5

STEP FIVE

Plan for annual renewal.

Certification is valid for 12 months. Renewal requires a new self-assessment, and scheme requirements can change between cycles.

- [ ] Diarise renewal at least four weeks before expiry to allow time for any required remediation.
- [ ] Before renewing, check the NCSC / IASME scheme requirements for any updates since your last certification.
- [ ] Conduct an internal review of your control state before submission. Last year's configuration may not meet current requirements.
- [ ] If your IT environment has changed significantly (new cloud services, remote-working changes, new software), update your scope documentation before renewing.

6

STEP SIX · OPTIONAL HIGHER TIER

CE+ track, if you need the higher tier.

CE+ adds independent technical verification by an IASME-approved assessor — not just questionnaire review. Standard CE is the first stage either way.

- [ ] Decide early whether CE+ is required. The standard CE process above is the first stage either way.
- [ ] Initiate CE+ within three months of standard CE certification. Miss the window and you restart the standard CE process. 3-MONTH WINDOW
- [ ] Confirm your ASP has qualified assessors able to conduct the CE+ technical verification.
- [ ] Prepare in-scope devices for hands-on testing, not just attestation.

CE vs CE+ at a glance

DIMENSION	CYBER ESSENTIALS	CYBER ESSENTIALS PLUS
Verification	Self-assessment questionnaire, reviewed by an ASP	Independent hands-on technical testing by an assessor
Five controls	All five must be met across in-scope systems	Same five controls, evidenced through testing
Timing	The first stage for everyone	Within three months of standard CE certification
Best for	Baseline assurance and most supplier requirements	Contracts or regulators requiring verified assurance

ONE PROCESS, TWO STAGES

You can't go straight to CE+. Standard CE certification comes first, then the independent technical verification. Plan both together so the three-month window doesn't force you to restart.

POWERED BY GRACIE

KNOW WHERE YOU STAND BEFORE YOU SUBMIT

Find your control gaps before your ASP sees a single answer.

Gracie AI Agents — with Personas and Skills — identify control gaps against all five Cyber Essentials requirements before submission, cutting evidence-collection time and removing the rework cycle from your certification process.

5/5	50–65%	Zero
Controls checked for gaps before you submit	Less time spent on evidence collection	Rework cycles after the ASP review

GUIDE	Cyber Essentials Checklist Guide	surecloud.com/resource-hub
DEEP DIVE	The Five Cyber Essentials Controls	surecloud.com/resource-hub
WALKTHROUGH	CE Questionnaire Guide	surecloud.com/resource-hub
HIGHER TIER	Cyber Essentials Plus Explained	surecloud.com/resource-hub

See SureCloud in action.

Gracie AI Agents and Skills automate the evidence collection, monitoring, and audit-trail work your certification demands — at scale.

Book a demo →