

Cyber Essentials readiness checklist

The UK government-backed scheme that certifies the five basic technical controls every organisation should have in place.

What Cyber Essentials asks

- ☐ Scope and boundary: Decide which devices, networks, people and cloud services are covered, and agree it with the certification body.
- ☐ Firewalls: Only necessary services reachable from the internet, on every in-scope device.
- ☐ Secure configuration: Remove unneeded accounts and software, change defaults and lock devices.
- ☐ Security update management: Supported software, automatic updates and critical fixes within 14 days.
- ☐ User access control: Approved accounts, unique credentials, MFA where available and separate admin accounts.
- ☐ Malware protection: Active anti-malware or allow-listing on every in-scope device.

Getting started

- ☐ Set your scope: Agree the boundary, including end-user devices and cloud services, and list what is in it.
 - ☐ Check the five controls: Compare each control with what you do today, using the free question set.
 - ☐ Choose your route: Go self-led through IASME, or use a certification body to help.
 - ☐ Complete the assessment: Answer the questions, have a board member or equivalent sign off, and respond to the assessor.
 - ☐ Consider the Plus level: Book independent technical testing if customers need stronger assurance.
-

Official source

[ncsc.gov.uk/cyberessentials/](https://www.ncsc.gov.uk/cyberessentials/) - <https://www.ncsc.gov.uk/cyberessentials/overview>

Want a scored report by email? Run the free assessment at

<https://www.optimuscyberx.ai/frameworks/cyber-essentials/assessment/>