Cyber Essentials readiness checklist

Woodruff Training • woodrufftraining.com

Cyber Essentials asks you to have five basic controls in place. None of them are exotic, and most small businesses are already part of the way there without realising. Work through the questions below to see where you stand before you pay for an assessment.

Please read. This is a preparation aid, not the official Cyber Essentials self-assessment. Working through it does not certify your business and does not guarantee you will pass. Certification is awarded by a certification body licensed by IASME, who run the scheme on behalf of the NCSC.

BEFORE YOU START

Know what you are certifying

Assessments come unstuck on scope more than anything else. Work out what is included before you answer a single technical question.

- [ ] You have listed every laptop, desktop, tablet, phone and server the business uses.
- [ ] That list includes devices staff use from home, and their own phones if they read work email on them.
- [ ] You have listed your cloud services: email, file storage, accounting, anything staff log into.
- [ ] You have decided whether the whole organisation is being certified, or a clearly defined part of it.
- [ ] Somebody owns this piece of work and has the time to see it through.

CONTROL 1

Firewalls

Something has to sit between your devices and the internet, deciding what is allowed through.

- [ ] Every device that connects to the internet is behind a firewall, either the one in your router or the software firewall built into the device.
- [ ] Staff working from home or on public Wi-Fi have the firewall on their own device switched on.
- [ ] The default administrator password on your router or firewall has been changed to something long and unique.
- [ ] The firewall settings cannot be reached from the internet, or are protected by multi-factor authentication if they have to be.
- [ ] Every rule that opens a service to the internet has a business reason you could explain, and rules you no longer need have been removed.

CONTROL 2

Secure configuration

Devices and software arrive set up for convenience rather than safety. This control is about tightening them before use.

- [ ] Default passwords on new devices, software and accounts are changed before anyone uses them.
- [ ] Software, apps and accounts nobody needs have been removed or disabled.

- [ ] Devices lock themselves after a short spell of inactivity and need a password, PIN or fingerprint to wake.
- [ ] Screen unlock uses a PIN or password long enough to be a real barrier, on a device that limits repeated guessing.
- [ ] Auto-run is switched off, so a USB stick cannot launch software the moment it is plugged in.

CONTROL 3

Security update management

Most successful attacks use a flaw that was fixed months ago on machines that never took the fix.

- [ ] Operating systems and applications update automatically wherever that option exists.
- [ ] Somebody checks that updates have actually installed, rather than assuming they have.
- [ ] Security updates rated critical or high risk are applied within 14 days of release.
- [ ] Software the vendor no longer supports has been removed or replaced.
- [ ] Devices too old to receive security updates have been retired or taken off the network.

CONTROL 4

User access control

People should have the access their job needs, and no more. Administrator rights are the ones that matter most.

- [ ] Every person has their own account and nobody shares a login.
- [ ] New accounts are approved by someone before they are created.
- [ ] Accounts are disabled the day a person leaves.
- [ ] Administrator accounts are used only for administrator work, with a separate ordinary account for email and browsing.
- [ ] You review who holds administrator access at least once a year and remove anyone who no longer needs it.
- [ ] Multi-factor authentication is switched on for your cloud services and for every administrator account.

CONTROL 5

Malware protection

Something needs to stop malicious software running, whether that is anti-malware or only permitting approved applications.

- [ ] Every device is protected, either by anti-malware software that updates itself or by only allowing applications from an approved list or official store.
- [ ] Anti-malware software scans files as they are opened rather than only on a weekly sweep.
- [ ] Staff are warned before visiting websites known to be malicious.
- [ ] Staff know how to report a device behaving strangely, and who to tell.

Backups are not part of Cyber Essentials, which surprises people. They are still the thing that decides how bad a ransomware morning gets, so keep a copy of your data somewhere separate and test that it restores.

Stuck on a few of them? We go through the gaps with you and get you ready to apply. woodrufftraining.com