arcsystems

Cyber Essentials certification:
The essentials

A quick, concise guide to help you become Cyber Essentials certified.

Why would you want cyber essentials?

How does Cyber Essentials assess a business?

How do you compare?

How do you improve?

How can Arc help you achieve certification?

Why your business needs Cyber Essentials

With only 5% of businesses holding a Cyber Essentials certification, it's safe to assume that the majority of people reading this will work in a business that isn't certified. Given the staggering global cost of cybercrime, currently standing at £6.53 trillion and predicted to escalate to £11.1 trillion by 2028, it becomes clear that obtaining a cybersecurity certification is not just essential, but an absolute necessity.

Certification brings benefits that go beyond just peace of mind and cost savings from continued protection. It automatically includes cyber liability insurance for UK organisations with turnovers up to £20 million. By getting certified, your business not only stands out but also builds a stronger reputation, increasing customer confidence and loyalty.

On top of that, being listed in the Cyber Essentials directory is essential if you want to tender for some national and even local government contracts, including for the MOD, and the NHS. Despite that, only around half of businesses know the Cyber Essentials certification exists.

Maybe Cyber Essentials is something you're considering, perhaps you feel an urgent need to get certified, or maybe you're somewhere between the two. Wherever you fall, this handbook will help you make sense of what a Cyber Essentials assessment measures, find out how close you are to meeting its requirements, and establish what you need to do to get there.

Cyber Essentials: The Basics

Cyber Essentials, in their own words, is “an effective, government backed minimum standard scheme that will help you protect your organisation, whatever its size, against a whole range of the most common cyber attacks”.

The National Cyber Security Centre, which runs the Cyber Essentials Scheme, describes most cyber crime as “the digital equivalent of a thief trying your front door to see if it’s unlocked”. Essentially, Cyber Essentials certifies that a business has its digital doors locked.

That’s a level of security any business would want to have (hence the name ‘Essentials’), and you can see why prospective customers could prefer a partner who has the certification over one who doesn’t, and why some organisations expect it before a business can pitch or bid for work.

So, what are the essentials of Cyber Essentials?

1. **Firewalls**
2. **Secure configuration**
3. **User access control**
4. **Malware protection**
5. **Security update management**

Firewalls

Security systems that monitor traffic to your server network according to security rules.

- Change the default admin password, and the new one must be hard to guess.
- Your firewall cannot allow administrative access from the internet, except for documented business needs. In that case, it either needs a Multi-Factor Authentication login, or a small list of trusted IP addresses that can access it (with a password).
- The firewall must block unauthenticated inbound connections.
- An authorised person must approve all rules for inbound connections, document those rules, and include the business need for each.
- Immediately remove access cases that are no longer required.
- Install firewall on devices that use (or may use) untrusted networks (e.g. public Wi-Fi).

Quick self-assessment

- [ ] Do you have firewalls between all systems and devices?
- [ ] Do you have a system for updating your firewall technology?
- [ ] Does your firewall include a remote working solution for hybrid workers?

Secure configuration

Think of this as the hygiene of your security — cleaning and tidying your systems.

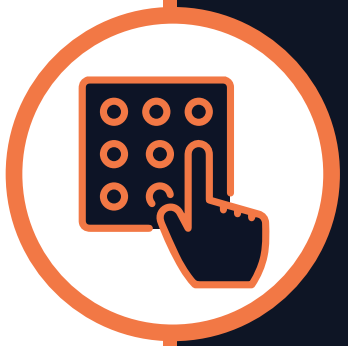
- Disable and delete unnecessary user accounts (like guests accounts and former employees' accounts).
- Replace all passwords that are easy to guess or discover (including all default passwords).
- Remove software and services that you don't need.
- Do not allow auto-run features (settings that allow file execution without authorisation).
- Make all data and services authenticate users before allowing access.
- Use device locking controls (e.g. device locks after 10 unsuccessful login attempts).

Quick self-assessment

- [ ] Do login PINs have at least 6 digits?
- [ ] Do your systems demand authorisations for all logins, downloads, and file executions?
- [ ] Have you disabled logins and accounts of former employees, contractors, and consultants?

User access control

All user access is controlled and protected, and no more users have access than are required.



- Set an approval process for the creation of user accounts.
- Give users unique credentials and base access on passwords or pins.
- Disable accounts after a defined period of inactivity, and when a user leaves the business.
- Remove privileged access when no longer necessary (e.g. after a change of role).
- Use multi-factor authentication (MFA), when possible (and always for cloud services).
- Create separate accounts that are for administrative tasks and nothing else (e.g. no web browsing or email accounts).

Quick self-assessment

- [ ] Have you disabled dormant, obsolete, and outdated user accounts and privileges?
- [ ] Have you separated your user accounts from your admin accounts?
- [ ] Do you have MFA where it's available?

Malware protection

Preventing malicious software from infiltrating your systems.

- Keep all anti-malware software up to date (update signature files at least daily).
- Configure software to scan files whenever accessed, downloaded, or opened.
- Scan all webpages for malware when accessed through a browser.
- Prevent access to malicious websites.
- List approved applications and prevent the installation of software that is not included.
- ‘Sandbox’ code with an unknown origin — run the code isolated from other resources.

Quick self-assessment

- [ ] Does your system scan all web pages and files before permitting access?
- [ ] Is all your malware protection software current?
- [ ] Can you isolate unknown or unfamiliar code from your system before you run it?

Security update management

All software (whether security-specific or not) should be always up to date.

- Ensure your software is all licensed by the provider.
- Ensure the provider is still supporting the software.
- Remove all software that is no longer supported.
- Update the software within 14 days of the update's release.
- Enable all available automatic updates.
- If the update requires manual configuration changes, apply those also within 14 days.

Quick self-assessment

- [ ] Is your software current (still receiving developer updates)?
- [ ] Do you have the latest version of all software that the business uses?
- [ ] Do you have a system to ensure the business installs all updates (including manual configurations)?

How do you become Cyber Essentials Certified?

How did you get on with the quick assessment? Whether you're self-assured in taking it on independently, or believe you have a way to go yet, Arc Systems is ready to assist you on the path to certification.

We'll start with our comprehensive cyber security review service, which will not only highlight recommendations but also outline any necessary adjustments required to meet the standards for Cyber Essentials certification.

Arc provides a breakdown of costs (including the assessment fee) and guide you through the journey to cyber security. The duration of this process can vary, spanning from a handful of weeks to a few months, dependent on the insights revealed during the review service.

Ready to become Cyber Essentials certified?
Book your cyber security review here.

arcsystems