Cyber Essentials
A guide for Law Firms
by
Cyber Security Partners

All businesses are at risk of cyber attack. The UK government backed Cyber Essentials is a cyber security guide for all businesses. Successful implementation protects against 80% of the most common attacks.

Law firms are very attractive targets for cyber attackers as they handle confidential and sensitive information so Cyber Essentials is especially important for law firms.

Protect client data

Highly sensitive information, such as client records, legal documents, financial data and intellectual property, must always be protected.

Reputation matters

Data breaches and cyber incidents can significantly damage a law firm's reputation and can break client trust.

Win more business

The UK government requires all actual and potential suppliers to hold an up-to-date Cyber Essentials certificate. This requirement passes through to all your supply chain.

Trusted partners

Collaboration is key for a successful law firm. Demonstrate your commitment to cyber security to everyone within your eco-system.

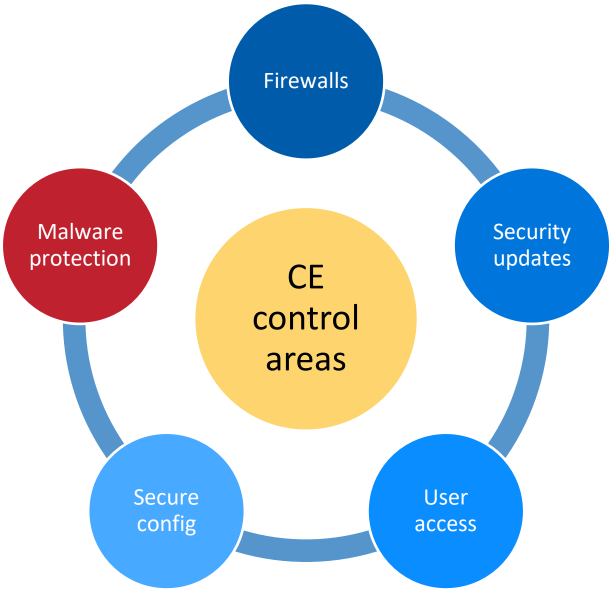
Regulatory requirements

Regulations are in place set by the SRA to ensure personal data is protected and law firms are insured. Cyber Essentials helps meet these requirements.

Cyber Essentials Overview

Cyber Essentials is a set of foundation level technical controls, across 5 major areas, to protect against the most common online security threats.

The certification was set up in 2014 by the National Cyber Security Centre and the UK government is pushing certification requirements through its entire supply chain. Private sector organisations must comply with these requirements to do business with Nuclear, Health, Education and Defence.

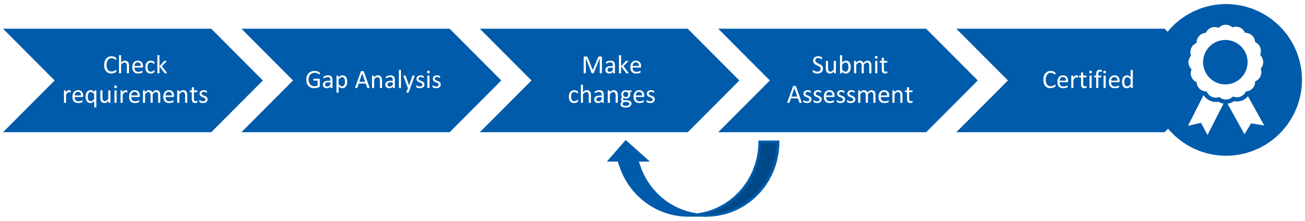


There are two types of Cyber Essentials that are available to customers to demonstrate your commitment to cyber security and data protection:

- Cyber Essentials - self assessed
- Cyber Essentials Plus - independently assessed.

Cyber Security Partners has gathered together 9 top tips to give some quick steps to review your cyber security posture or even move towards achieving certification against Cyber Essentials.

Cyber Essentials Certification Process



Check requirements

Gap Analysis

Make changes

Submit Assessment

Certified

CSP

CYBER SECURITY PARTNERS

Cyber Essentials Top Tips

Asset register 1

Create an asset register, listing all your laptops, desktops, mobile devices and software used. This will be used when checking the CE controls. Remove unused software.

Security policy 2

As a minimum, develop a security policy that outlines your approach to cybersecurity. It should cover data protection, access controls, incident response, and employee training.

Network 3

To protect against external attackers, implement network security measures such as firewalls and intrusion detection systems.

Training 4

Provide regular cybersecurity awareness training to all staff. Educate staff on best practices for password management, safe browsing habits and phishing awareness.

Patching 5

Check all your software, operating systems and applications are security patched to the latest version. Turn on auto-patching within 14 days where possible.

Cyber Essentials Top Tips

Multi-Factor Authentication (MFA) 6

Enable MFA on all devices and cloud services. MFA must be enabled for all users and administrators of your cloud services. Some exceptions are allowed.

User access control 7

Grant staff minimum privileges required to perform their role. User accounts must be pre-approved, disabled when no longer required and reviewed regularly.

Documentation 8

Create records of all cybersecurity policies, procedures, risk assessments and training records. These documents demonstrate commitment to good cybersecurity administration to clients and regulators.

Malware protection 9

Install anti-virus or anti-malware software on all devices to protect from internal and external attacks. Ensure auto-updates are activated for the latest protection.