Showing you're serious about

Cybersecurity

Cybersecurity in The UK's private sector

"Approximately 653,000 businesses (48%) have a basic skills gap. That is, the people in charge of cyber security in those businesses lack the confidence to carry out the kinds of basic tasks laid out in the government-endorsed Cyber Essentials scheme, and are not getting support from external cyber security providers. The most common of these skills gaps are in setting up configured firewalls, storing or transferring personal data, and detecting and removing malware"

- Cyber security skills in the UK labour market 2020, Department for Digital, Culture, Media & Sport

What is Cyber Essentials?

The UK Government Cyber Essentials accreditation provides reassurance that your organisation is taking proactive steps to combat cybercrime. You'll get a clear indication of how well armed you are against cyber threat.

Cyber Essentials

This self-assessment process provides a framework for ensuring the five key technical controls (secure internet connection, secure configuration, malware protection, user control and up-to-date devices and software) are correctly in place.

Once the survey is completed in the online portal, we'll audit the documentation.

Cyber Essentials Plus

Once you've achieved Cyber Essentials, you can progress to **Cyber Essentials PLUS certification.**

It's a thorough assessment of your organisation and includes a technical review of your infrastructure, with verification carried out by our Cybersecurity specialists remotely. The external vulnerability scan will include patch auditing, malware testing, web/email assessments.

The Five Cyber Essentials Technical Controls

The assessment reviews your business, its systems and procedures, against the following five technical controls:

Secure Configuration

Default configurations of new software and devices are set to be as easy as possible to connect and use, which creates vulnerabilities in your business' network if left unchanged. Settings should be checked, disabling and removing unnecessary functions and services, while default passwords should be updated before deployment. 2FA (Two-factor authentication) should be used for the most data sensitive accounts.

Secure Internet Connection

Creating a buffer between your IT network and other external networks, a firewall protects your internet connection, analysing incoming traffic to identify whether access should be allowed to your network..

User Access Control

In allowing access to those — and only those — accounts (software, settings, services and functions) that your people need in their specific job role, the risk of potential damage can be minimised.

Up-To-Date Devices & Software

Operating systems and applications become vulnerable if they are not up kept to date. In order for patches, whether new features or fixes to security vulnerabilities, to be applied, your operating systems, programmes, phones and apps should be set to “automatically update” where possible. When no longer supported, systems and applications should be considered for replacement.

Malware Protection

Malware, including ransomware and viruses, comes from a range of sources - infected email attachments, USB memory sticks, compromised home networks. Anti-malware measures are included within the most popular operating systems.

? Did You Know?

Around 80% of the most common cyber attacks can be prevented through the implementation of straightforward, affordable measurements that form the Cyber Essentials Scheme.

- Gov.uk, Cyber security boost for UK firms, Department for Business, Innovation & Skills

Cyber Essentials Pricing

Cyber Essentials

£300

Cyber Essentials Plus

£POA

Accreditation

Chess are acknowledged experts in the assessment of threat and vulnerabilities in IT estates.

We provide Cyber Essentials and Cyber Essentials Plus under the IASME consortium, the official government partner.

We're also certified by CREST which demands stringent standards, including appropriate levels of quality assurance processes; security controls; security assessment methodologies meeting CREST's additional qualification criteria; signing of an enforceable Code of Conduct and proven access to technically competent, qualified staff.

What our customers say about us?

”I’m very happy with our security now, it covers all the threats that you’d expect to see come from a technological point of view.”

Philips William & Co

“The presentation Chess did opened my eyes to this choice and with their virtual deployment options became a natural fit to replace our current solution.”

Progressive

“Chess staff are friendly, efficient and knowledgeable. I would highly recommend them.”

Clondalkin Agencies

About chess®

Chess is one of the UK's leading independent and trusted technology service providers, employing 480 skilled people across 6 UK sites, supporting a wide range of organisations.

By leveraging world-class technology, Chess helps you to connect your people, protect your data, grow your business, reduce your costs and work better together, which means your business, your people and your customers can thrive.

At Chess, we're passionate about our unique culture and our continuous investment in our people to be industry experts. We're extremely proud that our people voted us No.1 in 'The Sunday Times 100 Best Companies to Work for' list 2018, and we continue to celebrate more than ten years in the top 100.


WORK BETTER TOGETHER
PROTECT YOUR DATA
CONNECT YOUR PEOPLE
GROW YOUR BUSINESS
REDUCE YOUR COSTS
chess®
helps you

chess helps You

Protect Your Data

Contact Our Team Today

Marketing@ChessICT.co.uk

0330 107 1866

ChessICT.co.uk/

chess