secarma®
CYBERSECURITY EXPERTS

CYBER ESSENTIALS
&
CYBER ESSENTIALS PLUS

About the scheme

Let's start with the basics: Cyber Essentials is a UK Government backed scheme that is specifically designed for protecting organisations against common cyber-attacks.

Upon passing the scheme, your business receives a Cyber Essentials certification, a listing on the Cyber Essentials database, and you may also be entitled to Cyber Insurance. Cyber Essentials can be used either to certify your entire organisation, or it can be focused on a specific business unit provided that there is suitable network segregation.

The government took action in 2014 to reduce the security risk within their supply chain by introducing a mandate for any organisation embarking on a government contract to be certified against the Cyber Essentials scheme.

How can you benefit from Cyber Essentials?

Cyber Essentials was introduced by the UK government to help organisations mitigate 80% of cyber threats. The National Cyber Security Centre (NCSC) encourages all organisations that are based in or trading with the UK to implement either the Cyber Essentials or Cyber Essentials Plus scheme.

The areas of vulnerability that Cyber Essentials aims to assess include:

- Firewalls
- Secure Configuration
- Security Update Management
- User Access Controls
- Password Based Authentication
- Malware Protection

By implementing these technical controls, your organisation can defend itself against the most common cyber threats whilst being part of the endeavor to make the UK one of the safest places to do business.

Achieving Cyber Essentials Plus not only demonstrates an enhanced commitment to cyber security but also allows one of our technical auditors to review the implementation of security controls to ensure that they are in place and effective.

We provide

There are two levels to the Cyber Essentials scheme:

Cyber Essentials Basic

Cyber Essentials Basic requires you to answer a series of questions covering key aspects of your information security - this helps you to understand your organisations strengths and identify your weaknesses.

Cyber Essentials Plus

Once your organisation has Cyber Essentials Basic, you are able to apply for Cyber Essentials Plus. This involves a manual assessment of the technical controls and protections put in place within your organisation to secure it against common threats. Coupled with Cyber Essentials Basic, this provides a deeper assurance that your corporate data and vital systems are protected.

Please note that the prerequisite for obtaining the Cyber Essentials Plus certification is having achieved Cyber Essentials Basic certification within three months prior.

Pre-Assessment Consultancy

We provide a range of services to help strengthen your organisation's security posture before the assessment. Through our vISM services, one of our experts can help you meet specific security objectives: performing gap analysis, evolving your policy, processes and controls, and bringing you in line with the schemes expectations.

On Going Support

As well as completing the manual assessments, we are here to support you through the process of attaining your Cyber Essentials accreditations - this means helping you understand the requirements whilst providing advice and guidance on how to resolve any compliance concerns.

Post-Assessment Security Assurance

Using the information learned from your Cyber Essentials assessment, we can help build a structured security programme that will protect your organisation against a wide range of cyber threats. We're on hand as a trusted advisor to support all of your security objectives and requirements.

How it's delivered

Cyber Essentials Basic

Following any gap analysis work we've done together; you'll be given access to the Cyber Essentials self-assessment portal. From here, you will be able to view and answer the questions provided by the scheme, as well as input any additional notes where necessary.

We'll review your answers and, where necessary, provide feedback to indicate areas that may require additional attention, information, or remediation.

Once in compliance, we'll perform a final assessment of your answers, and you'll be granted a Cyber Essentials Basic Certification.

Cyber Essentials Plus

You must complete and achieve your Cyber Essentials Plus certification within 3 months of the date of your Cyber Essentials Basic certificate.

Cyber Essentials Plus involves a technical audit against the same controls that are applied during the Cyber Essentials Basic process. The Technical Audit is normally completed remotely but can be done on site on request.

We're on hand as a trusted advisor to support all of your security objectives and requirements.

Sampling

Where there is a large estate, Secarma will select a sample of end user devices and servers to perform internal testing on.

The sample size is pre-determined by IASME and is not negotiable. The sample must be representative of the entire organisation and will be determined based on what you tell us during your Cyber Essentials Basic assessment. When you book your Cyber Essentials Plus Audit, you will be given details of the required sample.

It's important to provide the full operating system version during your Cyber Essentials Basic application

In the context of Windows, this must include the edition and version eg. Windows 10 Pro 21H2

Please note that all operating systems must be actively supported by the manufacturer to be compliant with Cyber Essentials.

What to expect

On the day of testing, our expert assessor will complete the following activities

- External Vulnerability Scan of public facing IPs
- Internal Vulnerability Scan with credentials on a sample of end user devices and server
- Account Segregation Test on end user devices
- Anti Malware testing
- Review of MFA implementation

To achieve certification, all tests must be passed. Should any remedial work be required then you will have 30 days to make any changes and then undergo re-testing.

Working with you

In order for us to assess your organisation against Cyber Essentials Plus, you will need to provide the following

- Signed Authorisation for us to perform vulnerability scans.
- A list of your public facing IPs
- A Local administrator account on each of the devices in the sample
- WMI enabled and readable on Windows devices
- SSH access to any MacOS or Linux based devices
- Remote access to the devices in the sample. This is normally done by TeamViewer but we're happy to use your preferred remote access tool
- A teams call or screen sharing session with a sub-set of users as well as the administrators of all cloud services.

Our expert assessors and service delivery team will be on hand through the process to guide you through it but you must have sufficient technical resources available to configure the devices for scanning. Full instructions will be provided.

How to get started

Contact one of our account managers to get your quote today. Upon acceptance, you will be given access to our assessment portal where you can complete your Cyber Essentials Basic application.

Why Secarma?

Secarma consists of an experienced group of cybersecurity experts, highly skilled in penetration testing, training, and consultancy.

Drawing on experience gained over 20 years in business, and with a strong reputation to match, Secarma is the best choice for your cybersecurity needs;

We're continuously investing in research, internal training, and technical development to ensure we provide our customers with the best service.

Our consultative approach is how we stand out from the competition. We put you in touch with one of our experienced testers from the get-go, meaning you'll have an expert by your side throughout the process.

Our consultants are all highly accredited, passionate, and proficient not just at hacking into your systems, but also communicating to senior management and security teams how they achieved this.

By working with us, you can give your security team a better idea of what to expect, and prepare your business for real-world attacks.

Accreditations

Our experts pride themselves on their up to date certifications.

Your organisation's security and compliance are of top importance to us, which is why we've achieved the following accreditations:

nqa.
ISO 9001
QUALITY MANAGEMENT

nqa.
ISO 27001
INFORMATION SECURITY MANAGEMENT

CREST®

CERTIFICATION BODY
CYBER ESSENTIALS PLUS

Other services

With an ever expanding threat landscape, remote working, and GDPR regulations, cybersecurity services have never been more crucial for businesses.

Cybersecurity isn't a one size fits all process, and there are a number of options available to suit your needs and company objectives. Here are a few of ours:

Consultancy

We work with you to help you meet security objectives, develop your understanding of your organisation's security posture, test its defences, and prepare for worst-case scenarios.

Penetration Testing

A human-led simulation of a real cyberattack, designed to exploit your system's previously undetected vulnerabilities and determine the realworld risk to your business.

Security Training

Hands-on courses that teach you about security vulnerabilities and how to exploit them. We teach you how to break systems, then build them in a more resilient way.

Vulnerability Scanning

24/7 intelligent scanning that gives you a full overview of your current security posture, allowing you to track remediation, spot issues, and identify your areas of risk.

Contact Us

Get in touch with our experts today

0161 513 0960

secarma.com

enquiries@secarma.com

secarma®
CYBERSECURITY EXPERTS

WHAT WE DO

vISM

Training

Penetration Testing

Red Teaming

0161 513 0960

secarma.com

enquiries@secarma.com

secarma®
CYBERSECURITY EXPERTS