krome

# CYBER ESSENTIALS PLUS READINESS ASSESSMENT SERVICE

# CYBER ESSENTIALS PLUS

Cyber Essentials is a government and industry endorsed Cyber Security certification, its objective being to ensure that UK companies have a baseline level of security in place, which enables them to be more resilient to Cyber-Attacks.

Cyber Essentials comprises of six information security controls that provide the foundation of basic measures required to defend against the increasing threat of cyber-attack. The scheme's set of six critical controls is applicable to all types of organisations, of all sizes, giving protection from the most prevalent forms of threat coming from the internet.

Organisations can self certify as compliant for the basic Cyber Essentials certificate but to achieve the more highly regarded Cyber Security Plus Certification an external auditor will need to evaluate your security measures. You must be able to comprehensively demonstrate that you have the required level of protection in place against each of the six (previously five) security controls, with access control now split into two elements, comprising of user access and admin access control.

## CYBER SECURITY CONTROLS

### SECURE YOUR INTERNET

Ensure that you have correctly configured firewalls in place to prevent unauthorised access to your network and protect all of your devices that connect to the internet.

### SECURE CONFIGURATION

Secure your devices and software by ensuring that devices are properly configured and strong passwords are used to protect against potential vulnerabilities.

### ACCESS CONTROL USER & ADMIN

Control who has access to your data and services to authorised individuals on a required user/role basis. And appropriately manage privileged admin accounts.

### PROTECT FROM VIRUSES

Ensure that your network is effectively protected against viruses, malware, spyware, worms ransomware to prevent malicious code from causing damage or data breaches.

### KEEP UP TO DATE

Ensure that you have an effective and up to date patch management system/processes in place to apply security patches when available.

# HOW TO ACHIEVE CERTIFICATION

## Cyber Security Essentials: How to Achieve a Resilient, Certified, Cyber Security Strategy

The Cyber Essentials Plus certification can often be difficult and time consuming for companies to achieve without external objective help.

Working collaboratively with our clients, providing Cyber Security systems, compliance, policies and process assessments, we can give you a real time analysis and gap analysis of your Cyber Security landscape to fully prepare you for your Cyber Essentials Plus Certification.

### Utilise our external expertise.

With IT teams busy delivering projects or support, they often do not have the internal resource or time to keep on top of updating policy information, meaning that their policy documentation is often not representative of the actual processes that are in place.

It is also common to find that clients patch management solutions, although in place, actually require a more in-depth level of management than initially envisaged, to effectively avoid security vulnerabilities.

We have also found in the past that there can be areas of "Shadow IT" or systems outside of the IT departments control that are in scope for the Cyber Essentials Plus audit but have not been considered or effectively secured.

These are common challenges that we see within our client's environments, all of which become highlighted during the gap analysis phase of our Cyber Essentials Plus Readiness Assessment Service.

# CYBER ESSENTIALS PLUS

## Cyber Essentials Plus Readiness Assessment Service: Cyber VALIDATE

### Process Review, Gap Analysis and Compliance Consultancy

**1**

**INITIAL SCOPING CALL**

An initial scoping call will be required to ascertain the size of environment, identify all sites, data centres and any specific target areas for concern within the six cyber essential controls.

**2**

**DISCOVERY - *1 DAY ON-SITE/OR REMOTE WORKSHOP**

Individual heads of departments are required to discover and understand all aspects of potential exposure. The IT department will need to divulge information on all firewalls, systems, security measures, policies and management processes. The full scope for assessment is defined from the workshop so it is important to have the right people involved at this stage. Data is complied to build a complete security landscape picture.

**3**

**GAP ANALYSIS - *5 DAYS ON-SITE/OR REMOTE**

Using the information gathered at the workshop, a gap analysis will be performed with a defined list of specific questions, in line with the 6 security control. Working with the people in the business that are responsible for each area we will complete the questions and will categorise the responses by using a Red, Amber and Green rating to produce a report detailing the responses and the required actions for compliance for each response.

**4**

**REMEDIATION REPORT**

Using the data we will create an in depth managerial level report, showing who has been involved, all of the data that has been compiled and any immediate areas of concern. We will also compile an "Evidence Locker" containing all of the information gathered. The report is sectioned to relate to each of the 6 cyber essentials controls and provides an easy to digest summary of the requirements needed to meet compliance per each control.

**+**

**OPTIONAL: REMEDIATION IMPLEMENTATION**

Once we have presented our full report back to you, we can provide you with the recommended remediation actions and information required to implement the changes yourselves or we can work with you to implement the solutions or changes required under a separate project

*Timescales quoted are subject to change based on the output of the scoping call.

# CYBER ESSENTIALS PLUS

## Advanced Cyber Essentials Plus Readiness Assessment Service: Cyber MITIGATE

### Advanced Vulnerability Assessment

In addition to our standard Cyber Essentials Plus Readiness Assessment Service, we can also provide an added level to the service in the form of an Advanced Vulnerability Assessment. Using our portfolio of Cyber Security products we will deploy specific Cyber Security analysis tools to scan your environment for internal and external vulnerabilities to highlight any areas of weakness.

**1**

#### VULNERABILITY SCAN

Using Approved Scanning Vendor Tenable we will initiate an internal and external vulnerability scanning assessment which will identify any areas of weakness, including software flaws, missing patches, malware and misconfigurations across a variety of operating systems, devices and applications.

**2**

#### FIREWALL ASSESSMENT

Using a pre-configured Palo Alto Networks firewall device, we can passively inspect and analyse your traffic in a non-intrusive manner. Providing detailed information on how many known and unknown threats were identified, what applications are delivering malware/exploits, identify high-risk processes and applications, and provide an overall check on the effectiveness of your current Firewall.

**3**

#### PRIVILEGED ACCOUNTS & PASSWORD ASSESSMENT

Using discovery tools from Thycotic we will assess the current levels of password security and the policies around them. We will provide you with a summary of any users that are using insecure passwords, expired passwords, any privileged accounts, admin accounts who are unknown, left or should not have privileged account access.

**4**

#### VULNERABILITY REPORT

After applying these tools in your environment we will provide a report summarising all of the security vulnerabilities discovered via the three assessment tools and will provide a suggested plan for resilience improvement and compliance across all areas reviewed.

**+**

#### OPTIONAL: REMEDIATION IMPLEMENTATION

Should you wish to implement the full versions of any of the products that we have used at the assessment stage, Krome can work with you to implement the required solutions under a separate remediation project.

# CYBER ESSENTIALS PLUS

## Assessment Completed:
## Cyber Essentials Plus Certification Ready?

We've completed the assessment, any remediation has been made and your RAG list is now Green for Go!

So how do you become Cyber Essential Plus certified?

You will now need to appoint a certified auditor to perform your evaluation and award your Cyber Essentials Plus Certification, you will find the full approved Directory of Accreditation bodies here. We can also recommend someone should you wish us to.

The Cyber Essentials Plus certification body will provide you with a questionnaire to complete, they will all require you to supply various forms of evidence to verify that your IT is suitably secure and meets the standards set by Cyber Essentials Plus.

Throughout our Cyber Essentials Plus Readiness Assessment Service we will have complied an "Evidence Locker" for you, which contains all of the documents, gap analysis, validations and the evidence provided, per control, to prove that measures are in place and each of the six controls have been met. This evidence locker can be submitted at auditing stage to validate compliance. Once you have submitted your evidence and questionnaire it usually takes around three days for the certification body to visit you, confirm compliance and award you your Cyber Essentials Plus Certification.

It is worth noting that our assessment and report will be correct at the time of completion. However, as processes and systems change within an organisation on a daily basis, it is not guaranteed that during the official audit stage, the auditor might raise additional areas for remediation before certification can be achieved.

Where we have been involved in the implementation of any remediation activity or the implementation of systems, should the external audit find any issues with our remediation work, we will guarantee to resolve it for you, in order for you to obtain certification.

# CYBER ESSENTIALS PLUS

## Maintaining Cyber Essentials Plus Certification

### You've ticked all of the boxes, you're fully compliant and you've obtained your official Cyber Essentials Plus Certification!


But what do you need to do to maintain it?

At this stage your organisation is certified as Cyber Security Essentials Plus compliant and you are now officially recognised as a business that takes Cyber Security and the protection of data seriously. Unfortunately, but understandably, it doesn't validate you forever, the UK Government recommends that all businesses renew their security measures and their certification annually to effectively continue to avoid security vulnerabilities and ensure compliance standards within the six controls remain.

At the renewal point we offer an Annual Health Check assessment service which is started approximately 6-8 weeks before the re-certification date. At this stage we can usually offer a shorter, 2-day assessment period, comprising of a 1-day review and 1-day reporting to ensure that all previous assessed controls are still compliant and highlighting any new or additional remediation requirements. This would of course be subject to review, should any significant changes, additional sites, new datacenters, business acquisitions or mergers for example could all affect the time required for re-certification assessment.

Any elements of the service that are under a managed service from Krome will remain compliant throughout the year, any that are managed internally will be assessed during the health check.

To discuss any element of our Cyber Security Plus Readiness Assessment service please contact us on 01932 232345 or email sales@krome.co.uk.

Krome Technologies Ltd
Head Office: Krome House Pound Road Chertsey Surrey KT16 8ER Tel:01932 232345
Manchester Office: Krome House Quays Reach Salford Manchester M50 2ZY Tel: 0161 868 1360
www.krome.co.uk | sales@krome.co.uk

krome