HOW TO BECOME A **CYBER ADVISOR**

The new NCSC scheme to help small and medium organisations access consistent, high quality cyber security advice.

NI Cyber Security Centre

IASME CONSORTIUM

National Cyber Security Centre

TABLE CONTENT

ABOUT THE CYBER ADVISOR SCHEME

IASME is partnering with the National Cyber Security Centre (NCSC) to deliver the Cyber Advisor scheme. It provides small and medium sized organisations with reliable and cost effective cyber security advice and practical support.

In the past organisations seeking help from an NCSC approved cyber security expert tended to have complex and high risk cyber security requirements including, but not limited to, governments, wider public sector and Critical National Infrastructure. If your requirements are complex or you operate in a nationally critical sector, , see the NCSC Assured Cyber Security Consultancy scheme pages. Scan QR code for more information;

Today, expedited by the pandemic, the widespread adoption of digital technology for products and services has made basic cyber security essential to every business that connects to the internet. Accessibility to this protection contributes to the national security of the UK. Consequently, the NCSC aims to extend their assurance to trusted sources of cyber security advice aimed at small and medium size organisations.

Despite a growing emphasis on cyber security, many organisations often find it hard to choose the right help to meet current guidance. The Cyber Advisor scheme aims to enable customers to trust providers of cyber security advice and their implementation of that advice.

HOW DOES IT WORK

Cyber Advisors will initially focus on helping organisations to implement the five Cyber Essentials Technical Controls. This service will be known as Cyber Advisor (Cyber Essentials). The name includes Cyber Essentials in order to differentiate them from any future assured Cyber Advisors assisting small organisations in other areas of cyber security.

The Cyber Essentials standard has been adopted because the NCSC recognises this as a good baseline standard that defends against a range of commonly experienced cyber attacks, including ransomware attacks.

Cyber Advisors (Cyber Essentials) can help organisations assess the gap between their current cyber security stance, and that achieved by implementing the Cyber Essentials technical controls. This service is tailored towards small and medium sized organisations and the Advisors have all been assessed not just on their technical knowledge, but also their ability to work specifically with small organisations.

With the specific needs of an individual business in mind, Cyber Advisors can provide hands-on support to help the organisation take recommended actions.

An organisation will be helped to meet the Cyber Essentials technical controls, however, they do not necessarily need to be aiming for Cyber Essentials certification. The advice offered by Cyber Advisors will help prepare an organisation should they wish to certify, in which case, they will need to apply through a Cyber Essentials Certification Body.

WHAT IS THE DIFFERENCE

BETWEEN A CYBER ESSENTIALS CERTIFICATION BODY AND A CYBER ADVISOR ASSURED SERVICE PROVIDER?

A Cyber Essentials Assessor works for a Certification Body. They can assess whether or not an organisation meets the criteria required for Cyber Essentials certification and issue that certification – something a Cyber Advisor cannot do unless their organisation is also a Cyber Essentials Certification Body.

For more information on how to become a Cyber Essentials Assessor and how your organisation can become a Certification Body follow the below QR code or click here;

A Cyber Advisor works for an Assured Service Provider. They are competent at offering practical, hands-on IT configuration and support for implementing the Cyber Essentials technical controls and have a proven ability to understand and work with small organisations.

HOW DO I BECOME A CYBER ADVISOR?

The Cyber Advisor scheme provides small and medium sized organisations with reliable and cost effective cyber security advice and practical support.

The scheme allows the NCSC to recommend independently assured organisations to consumers, so they can have confidence in buying cyber security advice. For those providers already doing this type of work, the Cyber Advisor scheme aims to recognise your competence.

To become a Cyber Advisor (Cyber Essentials), you will need to pass an independent assessment, the **Certificate of Competence in Cyber Essentials Implementation** and provide IASME with that evidence. You will then be required to sit an online induction training course. The course will take you through the essential elements of the scheme and be followed by a simple test of understanding.

You can find more information on the Advisor Exam on the Cyber Scheme webpage or via this QR code:

Please note, all Cyber Advisors (Cyber Essentials) must be based in the UK or Crown Dependencies.

Once an individual has successfully passed the Cyber Advisor (Cyber Essentials) exam, the company they work for can become an NCSC **Assured Service Provider.**

What are the benefits of becoming a Cyber Advisor and why become one?

The Cyber Advisor scheme allows the NCSC to recommend independently assured organisations that can help their customers implement a baseline level of cyber security. By creating a trusted ecosystem, consumers will know better who to engage and what to expect. Furthermore, for those already doing this work, the Cyber Advisor scheme aims to recognise their competence.

HOW TO PREPARE FOR THE ASSESSMENT

The NCSC recognises that the 'Certificate of Competence in Cyber Essentials Implementation' assessment assures businesses that the holder is competent to advise on and implement the requirements of the Cyber Essentials scheme. This certification is endorsed by the NCSC. NCSC also accredit the assessment bodies that run the assessments.

Prepare for the assessment

All applicants are responsible for ensuring they are ready for the assessment. Prospective applicants should self-assess against these requirements and only book the assessment once they meet them. Applicants should understand the following duties, knowledge, skills and behaviours.

Duties of the Cyber Advisor;

Conduct Cyber Essentials gap analysis.

Access the organisation and its internet-facing IT and identify where the organisation meets and fails to meet the Cyber Essentials controls.

Develop and present reports on the status of the Cyber Essentials controls.

Prepare a report for senior leadership detailing the requirements the organisation met and those that were not met. For the requirements not met, the report should explain why they were not met, the risk they pose to the organisation and recommended actions that should be taken.

Agree remediation activates for the Cyber Essentials controls.

Work with the organisation to agree on the remediation activities which should be implemented.

Plan remediation activities while remaining sympathetic to operational activity.

Plan remediation activities that align to the risks and priorities agreed with the organisation.

Implement remediation activities while remaining sympathetic to operational activity.

Implement or guide technical teams in implementing remediation activities that align with the risk and priorities agreed with the organisation.

Develop and present post-remediation/engagement reports.

Either post-remediation or at the end of the engagement, prepare and present a report. This will summarise the engagement, detail remediation work completed, and point out any residual risk with recommendations for reducing those risks.

Knowledge Descriptions

A detailed understanding of the latest versions of the NCSC Cyber Essentials Requirements for IT Infrastructure.
Understand the NCSC Requirements for IT Infrastructure Document and how it applies to the business sector they are working in.

An understanding of the NCSC Small Business Guide: Cyber Security.
When working with small businesses/charities, Advisors should align the Cyber Essentials controls with the NCSC Small Business Guide and NCSC Small Charity Guide.

An understanding of the NCSC Cloud Security Guidance.
Cloud services are included within the scope of Cyber Essentials; advisors should be able to align those requirements with the NCSC Cloud Security Guidance.

Understand the basis of common threats and how they apply to small businesses.
Cyber Essentials is aimed at reducing the danger from common threats. The Advisor should distinguish between the different common threats and understand how they apply to the individual businesses.

An understanding of secure home and remote working approaches.
The NCSC Requirements for IT Infrastructure document describes the Cyber Essentials requirements in relation to home workers. Advisors should also understand how these relate to the NCSC guidance for home workers.

An understanding of secure development industry good practice guidance.
Bespoke components are outside the scope of Cyber Essentials assessments. However, the NCSC Requirements for IT Infrastructure Document recommends that such developments follow good industry practices and extensive testing. The Advisor should make recommendations from good practices such as OWASP* and recognised software development approaches.

*The Open Web Application Security Project (OWASP) works to improve the security of software through community led open-source projects, more details can be found here.

Knowledge of gap analysis frameworks to help organise work.
Gap analysis frameworks will allow Advisors to plan their work effectively.

The application of the Cyber Essentials technical controls to common approaches.

Understand how to apply the Cyber Essentials controls to commonly used platforms. This knowledge can include understanding relevant and reliable information sources that provide instructions for device configuration.

Understanding of dependencies between each of the Cyber Essentials controls

When planning implementation or negotiating appropriate controls actions the Advisor will need to understand any dependencies between the Cyber Essentials controls. For example, when implementing password policies this should be done in line with both Secure Configuration and Access Management.

Information sources relevant to implementation of Cyber Essentials controls

Be able to reference reliable sources of information which relate to the implementation of Cyber Essentials controls. These may be NCSC resources or other industry resources.

Understanding business and technical dependencies relevant to the implementation of Cyber Essentials controls

Be able to develop and execute a remediation plan which aligns to any technical dependencies between controls and one that causes minimal disruption to the running of the business.

Skills Descriptions

- Organisation and planning
- Negotiation
- Communication
- Investigation/Audit
- Ability to explain technical requirements in non-technical language
- Record keeping
- Ability to identify appropriate and proportionate approaches for a business to mitigate the identified gaps in the Cyber Essentials Requirements
- Report Writing
- Presentation
- Ability to understand organisation priorities of clients

Behaviour Descriptions

- Professional approach
- Collaborative approach
- Non-judgemental

Structure of Assessment

The overall aim of the assessment is to ensure that applicants have demonstrated the necessary competencies to successfully perform the duties of a Cyber Advisor.

Applicants will be presented with real-life organisational scenarios and will be required to understand the organisation and any issues it may have in achieving compliance with the Cyber Essentials controls. During the assessment, applicants may be asked to:

- present findings
- present options
- plan implementation activities
- work with customers or their representatives to implement solutions

The exam will consist of multiple choice, a written section and an interview with role play elements. Throughout the process, assessors will observe applicants and will note applicants' responses to the requirements of the assessment. To ensure fairness of the assessment, assessors will be provided with reference material to assess applicants against. Assessments will typically take 2-3 hours.

CYBER ADVISORS CAN HELP ORGANISATIONS BY

With the specific needs of an individual business in mind, Cyber Advisors can provide hands-on support to help the organisation take recommended actions.

- Conducting Cyber Essentials gap analysis to assess the organisation's internet-facing IT, identifying where it fails to meet the Cyber Essentials controls.
- Developing reports on the status of the organisation's Cyber Essentials controls i.e. detailing the requirements that are met and those that are not; describing why controls are not met and the risks the organisation is exposed to; recommended actions to take.
- Working with the business to agree remediation activities.
- Planning remediation activities that align to the risk and business priorities.
- Implementing remediation activities – or guide technical teams to do so – sympathetically to operational activities.
- Developing and presenting post-engagement reports summarising the engagement and detailing any remediation work completed, pointing out any residual risk with recommendations for reducing those risks.

Any organisation can find a qualified and approved Cyber Advisor working within companies assured by the NCSC. This makes it simple for organisations that are starting out on their cyber security journey to benefit from expert skills and advice offered by qualified individuals at a cost to the organisation.

HOW DO I BECOME A NCSC ASSURED SERVICE PROVIDER?

To offer NCSC assured Cyber Advisor services, your organisation will need to become an Assured Service Provider registered with our scheme delivery partner, IASME.

You will also need to employ at least one formally assessed Cyber Advisor. Similarly, a Cyber Advisor must have passed the assessment and be employed by an Assured Service Provider before they can offer NCSC assured Cyber Advisor services.

Companies of any size can apply to join the scheme and we welcome those located in or serving geographically remote or underrepresented areas.

When applying to be an Assured Service Provider, organisations will be expected to meet requirements demonstrating good cyber security and a commitment to achieving an excellent and consistent customer experience. You will also need to have Cyber Essentials certification.

All Cyber Advisors need to be part of an Assured Service Provider organisation to be able to carry out assured Cyber Advisor services.

All Assured Service Providers have to show they meet both security and quality requirements.

They can do this by holding one of these security certifications.

- UKAS-accredited ISO 27001 certification
- Audited IASME Cyber Assurance (Level 2) certification

They also need to hold one of these quality requirements:

- UKAS-accredited ISO 9001 certification
- IASME Quality Principles alongside an IASME Cyber Assurance (Level 2) certification
- QG Quality Fundamentals+ certification

An NCSC Assured Service Provider must also:

- Provide independently verified evidence that they have achieved and maintain Cyber Essentials
- Sign and return the associated contract
- Employ at least one individual who has passed the Cyber Advisor assessment
- Pay an annual subscription fee

If your company is interested in becoming an NCSC Assured Service Provider, please contact us at info@iasme.co.uk.

www.nicybersecuritycentre.gov.uk
info@nicybersecuritycentre.gov.uk

NI Cyber Security Centre

IASME CONSORTIUM

National Cyber Security Centre