Delivery Partner

in association with National Cyber Security Centre

Cyber Advisor Assessment Provider

# CYBER ADVISOR

## (CYBER ESSENTIALS IMPLEMENTATION).

TESTING THE KNOWLEDGE OF THE CYBER ESSENTIALS STANDARD, AND THE PRACTICAL SKILLS REQUIRED TO IMPLEMENT ANY RECOMMENDATIONS MADE.

**The Cyber Scheme Cyber Advisor Assessment: Exam Objectives and Syllabus Version 1.0**

# ABOUT THE EXAM

**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 and the value of certification. This certification is endorsed by the NCSC and is managed to their high standards.**

The Cyber Scheme has been licensed as an Assessment Provider by IASME, who are operating the scheme on behalf of the NCSC. NCSC assured Cyber Advisors will have to pass our assessment. This measures your:

- Knowledge and understanding of the Cyber Essentials' technical controls
- Competence in providing practical, hands-on support
- Ability to understand and work with small and medium sized organisations.

There are no prerequisite qualifications for becoming a Cyber Advisor, although it has been found that candidates are more successful in the assessment if they have several years experience in IT, cyber security, and providing consultancy to different types and sizes of business.

## Assessment requirements

**The assessment process is made up of three elements: multiple choice test; questions requiring short form written answers and a face-to-face discussion with an assessor.**

The assessment tests your knowledge of the Cyber Essentials Standard and the practical skills required to implement any recommendations made to organisations who wish to meet the Standard.

**To become a Cyber Advisor, you will need to:**

- Pass the assessment, at which point you will be issued with a Certificate of Competence in Cyber Essentials Implementation
- You will then need to provide IASME with that evidence.
- Once that is submitted, you will be required to sit an online induction training course with IASME, which will take you through the essential elements of the scheme and be followed by a simple test of understanding.

# DUTIES OF THE CYBER ADVISOR

**A Cyber Advisor will be expected to carry out the following tasks once qualifid. These will be assessed during the exam process.**

**Conduct Cyber Essentials gap analysis**

The advisor will assess the organisation and its internet-facing IT identifying where the organisation meets and fails to meet the Cyber Essentials controls.

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

After completing a gap analysis, the advisor will prepare a report targeted at senior leadership within a business, detailing the Cyber Essentials requirements that are met and those that are not met. For those not met, the report will describe why the control is not met, the risks the business are exposed to, and the recommended actions the company should take.

**Agree remediation activities for Cyber Essentials controls**

The advisor will work with the business, its IT Team (if they have one) and the senior leadership team to agree on the remediation activities which should be implemented.

Plan remediation activities sympathetically to operations activities

The advisor will plan remediation activities that align to the risk and business priorities agreed with the senior leadership team.

**Implement remediation activities sympathetically to operational activity**

The advisor will implement or guide technical teams in implementing remediation activities that align with the risk and business priorities agreed with the senior leadership team.

**Develop and present post-remediation/engagement reports**

Either post-remediation or at the end of the engagement, the advisor will prepare and present a report aimed at the business's senior leadership team; this will summarise the engagement, detail any remediation work completed, point out any residual risk with recommendations for reducing those risks.

# ASSESSMENT CRITERIA .1

**Our assessment criteria will ensure that all the Knowledge Skills and Behaviours shown below are covered in the advisor assessments.**

## KNOWLEDGE DESCRIPTIONS

**A detailed understanding of the latest version of the NCSC Cyber Essentials Requirements for IT Infrastructure**

Advisors should 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**

Where advisors are working with small businesses, they should align the Cyber Essentials controls with the NCSC Small Business 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 businesses they are dealing with**

Cyber Essentials is aimed at reducing the threat from Common threats. The advisor should understand what Common threats are and how they apply to the business they are working with.

**An understanding of secure home and remote working approaches**

The NCSC Requirements for IT Infrastructure document describes the Cyber Essentials requirements regarding home workers. However, 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.

# ASSESSMENT CRITERIA .2

**Knowledge of current Cyber Essentials technical appropriate controls approaches**

Advisors should 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.

**Implementing current Cyber Essentials controls**

Advisors should understand how to implement the Cyber Essentials controls within commonly used platforms.

**Information sources relevant to the implementation of Cyber Essentials controls**

The advisor should 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 CE controls**

The advisor should 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.

# ASSESSMENT CRITERIA .3

## SKILLS DESCRIPTIONS

**Organisation and planning**

The ability to prioritise, plan and organise any required activity.

**Negotiation**

The ability to be able to discuss options with clients and reach an outcome agreeable to all parties.

**Communication**

The ability to be able to communicate at the appropriate level depending on the audience.

**Investigation / Audit**

The ability to look for evidence of compliance or non-compliance with the Cyber Essentials controls.

**Ability to explain technical requirements in non-technical business language**

The ability to interpret technical information and present that to non-technical audiences.

**Record keeping**

Keeping good records both as evidence of the advisor's findings and for inclusion in reports.

**Ability to identify appropriate and proportionate approaches for a business to mitigate the identified gaps in the Cyber Essentials requirements**

Suggesting or implementing options that are appropriate for the business in question, not just suggesting the options they are familiar with.

**Report writing**

The ability to construct a report logically and professionally using appropriate language for the audience.

**Presentation**

The ability to present findings succinctly using language appropriate to the audience.

**Ability to understand business priorities of clients**

The ability to plan work in a manner that minimises business disruption.

# ASSESSMENT CRITERIA .4

## BEHAVIOUR DESCRIPTIONS

**Professional approach**

Behaviour that is appropriate to the working environment. Following professional code of conduct and ethical standards defined by the UK Cyber Security Council.

**Collaborative approach**

Working jointly with the customer or third parties to achieve the customer's objectives.

**Non-judgemental**

Working with the customer with an attitude that is open and not incorporating judgements of prejudicial views.

**Please visit thecyberscheme.org/cyber-advisor for extensive learning resources and to book your assessment.**