iasme

Guidance for the Cyber Advisor (CE) Assessment

Table of Contents

Introduction and Purpose

This document aims to assist individuals interested in pursuing the "Certificate of Competence in Cyber Essentials Implementation" exam to become a Cyber Advisor. In this document, we will explain the assessment process and requirements to help candidates prepare.

The Cyber Advisor scheme was established to help small and medium businesses find cyber security service providers with qualified individuals capable of providing appropriate guidance on implementing the Cyber Essentials controls.
Cyber Essentials is an effective, Government backed scheme that helps protect organisations, whatever their size, against a whole range of the most common cyber-attacks.

The scheme is called Cyber Advisor (Cyber Essentials) and the company assured by the scheme is an NCSC Assured Service Provider (Cyber Essentials) to distinguish them from other types of Cyber Advisor or Assured Service Provider. From this point in the document, we will just refer to Cyber Advisor and Assured Service Providers, but all are associated with the Cyber Essentials Scheme.

Understanding the Role of a Cyber Advisor

The primary role of a Cyber Advisor is to provide guidance on basic security requirements and assist businesses in implementing the Cyber Essentials controls. The Cyber Advisor helps organisations achieve compliance with Cyber Essentials, whether they aim to obtain certification or simply improve their cybersecurity practices.
This service is known as Cyber Advisor. Cyber Advisors can help organisations by:

- Conducting a Cyber Essentials gap analysis to review the organisation's IT and identify which changes are needed to meet the Cyber Essentials controls.
- Planning technical changes to improve security while being guided by an organisation's specific business needs.
- Carrying out the technical changes to improve security – or guiding the organisation's own staff to make these changes.
- Explaining clearly to the business owner what changes have been made and why, and what recommended changes need to be made.

It is important to note that a Cyber Advisor is distinct from a Cyber Essentials Assessor. Cyber Essentials Assessors work for a Certification Body and assess organisations applying for Cyber Essentials certification, but a Cyber Advisor is assured by the NCSC to deliver consultancy to small organisations

Qualifications and Eligibility

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 and cybersecurity.

Candidates must pass and maintain the "Certificate of Competence in Cyber Essentials Implementation" exam to be qualified as Cyber Advisors. Candidates must attend a Cyber Advisor Assessment Centre, managed by an Assessment Body, to sit the assessment. More details on the requirements and assessment process can be found below.

(The "Certificate of Competence in Cyber Essentials Implementation" is valid for three years. It is renewed by sitting the assessment again when the Certificate is due to expire. Cyber Advisors are also required to maintain their skills by continued professional development.
The Delivery Partner for the Cyber Advisor scheme will provide a policy detailing the continuing professional development requirements. The policy is planned to be implemented during 2024)

Practicing as a Cyber Advisor

How to become a Cyber Advisor

To practice as a Cyber Advisor, individuals must take the following steps:

1. Qualify to be a Cyber Advisor and provide a copy of the "Certificate of Competence in Cyber Essentials Implementation" to the Delivery Partner at training@iasme.co.uk

2. Work in the UK or Crown Dependencies

3. Be employed or contracted by an Assured Service Provider – an Assured Service Provider is an organisation that has proven their ability to deliver high-quality, tailored cybersecurity advice that meets the NCSC standard.

4. Sign a code of conduct for the Cyber Advisor scheme with the Delivery Partner

5. Complete an Induction programme, including Cyber Essentials update training, with the Delivery Partner

The organisation a Cyber Advisor works for must meet the requirements of an Assured Service Provider, and sign a license with the Delivery Partner, before an individual can join the scheme as a Cyber Advisor.

How to become an Assured Service Provider

Organisations that wish to become Assured Service Providers, to offer Cyber Advisor services, must apply to IASME at training@iasme.co.uk IASME are the Cyber Advisor Delivery Partner and run the scheme on behalf of the NCSC.

There are no restrictions on the size of the businesses that can become Assured Service Providers, however, the scheme is associated with advice for small businesses and so the organisation must already offer or plan to offer this service.

It is acceptable for organisations to offer both Cyber Essentials Certification and the Cyber Advisor Assured Service. It is not a requirement to offer both services. Some Certification Bodies offer consultancy on the Cyber Essentials certification process, but this is distinct from the Cyber Advisor Assured Service.

An organisation can become an Assured Service Provider by undertaking the following:

1. Employ or contract at least one qualified Cyber Advisor who has passed the "Certificate of Competence in Cyber Essentials Implementation" exam.

2. Hold and maintain a current Cyber Essentials certification.

3. Be domiciled in the UK or Crown Dependencies.

4. Hold and maintain commercial insurance certificates to the value of at least £1m.

5. Meet requirements demonstrating good cyber security standards. This can be achieved by holding one of the following security certifications:

   UKAS accredited ISO 27001* certification or
   IASME Cyber Assurance Levels 1 and 2

   * An ISO 27001 certificate that is not awarded by a UKAS accredited organisation is not accepted.

6. Meet requirements demonstrating good quality standards. This can be achieved by holding one of the following quality certifications:

   UKAS accredited ISO 9001* certification or
   QG Quality Fundamentals+ certification or
   IASME Quality Principles (achieved and audited as part of IASME Cyber Assurance Level 2 certification)

   *An ISO 9001 certificate that is not awarded by a UKAS accredited organisation is not accepted.

7. Sign a license to be an Assured Service Provider, with the Delivery Partner.

Duties, Knowledge, Skills, and Behaviours of a Cyber Advisor

The Duties, Knowledge, Skills and Behaviours describe what is expected of the Cyber Advisor role. The assessment is based on these expectations.

Duties (the role of the Cyber Advisor)

Duty		Explanation
D1	Conduct a Cyber Essentials' Gap Analysis.	Assess the customer organisation's current state and provide guidance on achieving compliance with Cyber Essentials'Requirements.
D2	Develop and present reports on the Cyber Essentials' Controls.	Prepare written and verbal reports on the organisation's compliance with the Cyber Essentials' controls.
D3	Agree on Remediation Activities.	Work with the organisation to determine appropriate and proportionate actions to address gaps in the Cyber Essentials controls.
D4	Plan Remediation Activities.	Understand what needs to be done and the dependencies on business activities. Plan sympathetically to the business' operational activities.
D5	Implement Remediation Activities.	Execute the planned remediation activities.
D6	Develop and Present Post-Remediation Reports.	Assist the organisation to become self-sufficient and understand how to maintain their cybersecurity levels. Provide reports detailing the work done, its importance, and the required maintenance. Use appropriate business language, not technical language.

Knowledge (what the Cyber Advisors needs to know)

	Knowledge Area	**Explanation**
K1	Detailed understanding of the latest version of the NCSC Cyber Essentials' Requirements for IT Infrastructure.	The Cyber Essentials' controls and guidance are documented in the NCSC Requirements for IT Infrastructure document. Without a detailed understanding of this, advisors will not understand the requirements. The latest version can be located on the NCSC website https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure- v3-1-January-2023.pdf
K2	An understanding of the NCSC Small Business Guide: Cyber Security.	The Cyber Advisor will be focused on Small and Medium (SME) businesses. This guide complements Cyber Essentials and will help in identifying appropriate and proportionate implementation of the controls.
K3	An understanding of the NCSC Cloud Security Guidance.	Many organisations now rely on cloud solutions, so an understanding of this guidance is useful.
K4	Understand the basis of common threats and how they apply to businesses they are dealing with.	The advisor must understand the basis of the commodity-based threat. They should also be aware of any other threats a business they work with may be exposed to.
K5	An understanding of secure home and remote working approaches.	Home and remote working is now commonplace, so the advisor needs to understand the risks and relate these to the Cyber Essentials' requirements.
K6	An understanding of secure development industry good practice guidance.	Bespoke developments are outside the scope of Cyber Essentials. However, within the standard there is advice about bespoke development. The advisor must have enough knowledge of good industry secure development practices to be able to assist a business to implement appropriate processes.

K7	Knowledge of gap analysis frameworks to help organise work.	A gap analysis will most likely be the first stage of an advisor's engagement. They need to be able to articulate where the customer is in relation to the Cyber Essentials' requirements, and what work the business needs to do to close the gap. The GetReadyforCyberEssentials.IASME.co.uk website https://getreadyforcyberessentials.iasme.co.uk/ provides a good starting point for this.
K8	Knowledge of current Cyber Essentials appropriate technical controls approaches.	Not all businesses are the same. Therefore, the same solution for a Cyber Essentials' control will not work in all organisations. The advisor must be able to identify the right solution for a specific business.
K9	Understanding of dependencies between each of the Cyber Essentials' controls.	Organisations may need to implement the requirements in a certain way. The advisor should understand any dependencies between the controls which may influence how they are implemented within a particular business.
K10	Implementing current Cyber Essentials' controls.	At times the advisor may need to implement a control. They should either have the knowledge to do it, know reliable sources of information to inform them how to, know reliable resources who can do it on their behalf.
K11	Information sources relevant to the implementation of Cyber Essentials' controls.	It is accepted that an advisor cannot hold all the knowledge in their heads. However, they should be able to identify reliable sources of information to support their work.

K12	Understanding business and technical dependencies relevant to the implementation of Cyber Essentials' controls.	When implementing the Cyber Essentials' controls, there may be business dependencies to consider. The advisor should understand what is involved in implementing a control and how that may affect the business, to plan implementations that cause minimal disruption to the business.

Skills (what the Cyber Advisor does):

The Cyber Advisor should be proficient to act independently for each of these skills.

Skill		**Explanation**
S1	Organisation and Planning	The ability to plan and organise assignments effectively.
S2	Negotiation	Skill in negotiating appropriate control implementation and operational changes. Within any consultancy assignment, there will be a degree of negotiation. This could include negotiating on the most appropriate way to implement a particular control, or negotiating when an organisation's network can be taken out of operation to be modified. Negotiation includes discussion of options and reaching an outcome agreeable to all parties.
S3	Communication	Clear and concise communication using business language appropriate for the audience.
S4	Investigation and Audit	Assessing the current state of an organisation's cybersecurity using appropriate techniques.
S5	The ability to explain Technical Requirements	Ability to convey technical concepts in non-technical business language.
S6	Record Keeping	Maintaining records and submitting management information.

S7	Ability to identify appropriate and proportionate approaches for a business to mitigate the identified gaps in the Cyber Essentials' requirements.	Determining suitable and proportionate mitigation strategies for businesses that align to the Cyber Essentials' requirements.
S8	Report Writing	Providing written reports in a logical, professional manner using clear business language.
S9	Presentation	Delivering presentations using clear and concise business language.
S10	Ability to understand business priorities of clients.	Recognising and considering the priorities and context of client organisations.

Behaviours (How the Cyber Advisor carries out their duties):

Behaviour		**Further Information**
B1	Professional approach	Adhering to professional standards and ethical guidelines. A good reference for what is expected is the UK Cyber Security Council Ethical Declaration: https://www.ukcybersecuritycouncil.org.uk/ethics/ethi cal-declaration/
B2	Collaborative approach	Working with clients to find the best solutions that work for their business.
B3	Non-judgemental attitude	Avoiding judgment towards the client's operations or technology.

The Assessment Process

The assessment is designed to evaluate the candidate's knowledge, skills, and behaviours within a defined time frame. Over time there may be several Assessment Bodies (NCSC

Delivery Partners) for the Cyber Advisor Scheme, whose assessment approach is accepted by the NCSC. Any NCSC Delivery Partner and candidates can choose the one that suits their preferences, as the outcomes of the assessments will be considered equal. Assessment centres will be located throughout the UK, and candidates can book assessments through the respective assessment bodies' websites.

There is currently one Assessment Body – The Cyber Scheme https://thecyberscheme.org/

Current Assessment Details

The assessment lasts approximately two and a half to three hours. To allow for the pre-assessment administration, candidates should allow four hours in total. The assessment is open book, allowing candidates to use references during the assessment. All references used must be properly cited.
Candidates will be presented with real-life business scenarios. They will be required to understand the customer and any issues they may have in achieving compliance with Cyber Essentials' controls.

During the assessment, candidates may be asked to:

- Present findings
- Present options
- Plan implementation activities
- Work with customers or their representatives
- Implement solutions

Throughout the process, assessors will observe candidates and will note candidates' responses to the requirements of the assessment.

The assessment consists of two parts.

Part 1: Multiple Choice and Written Assessments

This section is completed through an online assessment portal, using a web browser. Candidates will be required to bring along their own laptop. This part of the assessment includes 12 multiple-choice questions and 12 short-form written answers. Candidates have two hours to answer the questions. The questions are based on a real-life business scenario, and candidates are encouraged to read the short-form questions carefully as they may not directly relate to the multiple- choice questions.
This part of the assessment evaluates:

- The candidates' understanding of the Cyber Essentials' requirements
- The application of the controls at an appropriate level for the business
- Use of reference sources
- Report writing skills

Part 2: Discussion with the Client

In this section, candidates engage in a 25 to 30 minute discussion with the assessor, who for the purpose of the exercise takes the role of the client. The assessor selects specific parts of the candidate's multiple-choice or short-form answers for further discussion.
The objective is to assess the candidate's technical knowledge, their ability to present technical information to a non-technical audience, their interpretation of the Cyber Essentials' controls, and their communication and negotiation skills.
This part of the assessment evaluates verbal communication skills, negotiation abilities, and presentation skills.

Question and Model Answer Example

Part One of the Assessment is the multiple-choice and short form written answer section. In this section, candidates should read the questions carefully. There is plenty of time. The short-form questions will be related to the multiple-choice question; and may extend the question further. The short-form written answer requires candidates to address the short- form question, not simply expand on the multiple-choice options and why an option was chosen. The example below illustrates this approach.

Example question

Multiple Choice –

What would a business do before installing a new router which contains a firewall?

A. Enter it into the asset register.
B. Change any default passwords.
C. Ensure everyone is off-line.
D. Check it is approved by the ISP.

Short form –

MotorMouth Inc. think they have changed the password on their BT router, but they have forgotten it. They ask you to provide guidance on what they should do. What would you advise.

The answer to the multiple-choice question is B. This is the only option that is a Cyber Essentials' requirement.

For the short form answer, candidates should document a plan, starting with the simplest of actions to the more radical. For each action, identify the pros and cons.
In this instance, the business only think they have changed the password, so it may be worth trying the default one as a first action. After that there would be the option of resetting the device to factory defaults, but here candidates would be expected to document what the effects of this would be. Finally, the most radical, costly and probably unnecessary approach would be to change the router, that is unless the router is no longer supported by BT, in which case it would need to be changed to comply with the Cyber Essentials' requirements.

Remember that it is not just technical knowledge being tested here. Think how to describe these options and how to describe the pros and cons. Ask yourself, could a non-technical person understand what you have said?
Scoring and Passing Criteria

Multiple-choice questions are scored based on correct answers, with candidates needing to achieve 80% accuracy to pass. For all multiple-choice questions, there is only one right answer. When looking at the options, candidates may need to use their judgement to select the best answer possible, as they may feel there is more than one correct answer. Failure in the multiple-choice section will result in an overall failure of the assessment, as it is assumed the candidate does not have the required level of Cyber Essentials knowledge. Short-form questions and the discussion are marked together, and candidates will need to score an average of 75% of the total marks for each part. There are a total of five marks available for each short-form question and each question covered in the discussion.

The assessor is looking for:

1. The response is factually accurate and reflects the current version of the NCSC Requirements for IT Infrastructure Document.
2. The response is communicated in clear, business English. Jargon is avoided or otherwise explained in simple terms.
3. The response contains added value, insight, or justification. This could include signposting the business to other NCSC guidance such as password, cloud, and small business. It could also include referencing other credible cyber security advice from other sources.

The assessor will mark answers as follows:

Assessor Score	Made up from	Assigned Mark
Insufficient	The answer contradicts current NCSC guidelines or fails to address points 1 and 2 above or is factually inaccurate.	0
Below expectations	The answer satisfies criteria 1 above	2
Meets expectations	The answer satisfies criteria 1 and one of the other criteria	4
Comprehensive	The answer satisfies criteria 1, 2, and 3 above	5

For the short-form answers, there are a possible 60 marks. The discussion has variable marks as the assessor will pick between 5 and 7 areas to explore further, however the average scoring is calculated on the number of areas covered.

Let's take the following scenario:

- For the short form there are a potential of 60 marks
- In the discussion, the assessor looks at 5 areas that will mean there are 25 marks available for the discussion.

The tables below show how the marking would work:

	Points	Percentage
All short form questions marked below expectations	24	40
All discussion questions marked below expectations	10	40
Average percent between Short form and discussion		40
Overall Grade Fail		

Table 1

	Points	Percentage
Short form: 10 Meets expectations 2 Comprehensive	50	83
Discussion: 3 Meets expectations 2 Comprehensive	22	88
Average percent between Short form and discussion		85
Overall Grade	Pass	

Table 2

In Table 1, the candidate has recited the Cyber Essentials' requirements and has not explained them in plain English. In this instance, they would fail the assessment.

In Table 2 the candidate has been awarded mainly good marks; this means they have recited the requirements and presented them in an appropriate manner for the scenario. In two areas they provided additional information, and this has resulted in a good pass.

Preparation and Tips for the Assessment Centre

The following is recommended to prepare for the assessment:

It is essential to be familiar with the latest version of the "Cyber Essentials Requirements for IT Infrastructure" document https://www.ncsc.gov.uk/files/Cyber- Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf
Candidates should ensure they understand and can demonstrate the duties, knowledge, skills and behaviours required of the Cyber Advisor.
Practice writing explanations of technical aspects using plain language and practice verbalising technical issues to non-technical individuals. It is a good idea to practice explaining the Cyber Essentials' controls to a non- technical family member.
Thorough preparation will enhance candidate performance during the assessment.

Remember that just reciting the Cyber Essentials' requirements will not be enough to pass the assessment centre. Candidates need to be able to apply the requirements appropriately to the organisation, considering the size, complexity, and budget. It is also relevant to be familiar with other guidance that sits alongside the Cyber Essentials' requirements. This could include NCSC Small Business Guide and other NCSC guidance, or other credible industry good practice like OWASP, or SANS for example.
When candidates are asked to give guidance or advice, this should be written as though they are writing to a client who may be non-technical. Candidates should write as if they are responding to an email or writing a paragraph for a report. Candidates should remember they are being tested as much on their written communications skills as their technical knowledge. It is possible to fail the assessment if technical knowledge is not communicated in plain business language.
The discussion is just that, a discussion. It is not an interview where candidates are just expected to answer questions. View it like this: A customer has been provided with a report or has been sent an email and they are asking for clarification. Candidates may need to ask follow-up questions to understand what the customer is having difficulty with and may have to present the information already presented in a different way. Communicate in a language that is appropriate to the role the assessor is playing i.e. the customer. Candidates may also need to ask clarifying questions or draw a diagram – if so, that's great. The discussion tests a candidate's verbal communication skills, negotiation skills, and presentation skills.

Reasonable Adjustments for the Assessment

If a candidate requires adjustments for exams due to special circumstances, these can usually be accommodated with prior notice. When booking the assessment centre, inform the assessment body of your requirements, and they will strive to meet them.

What to take to the Assessment

Candidates will be required to bring a valid proof of identity, which can be one of the following:

- UK photo driving license
- Passport
- Government issued photo ID

Candidates will require a device to access the online assessment, preferably this will be a personal computer, but a tablet would also work. If candidates have paper-based references, they can also bring those.

Further Information

For additional information about becoming a Cyber Advisor, candidates can refer to the provided references or contact the relevant organisations via the provided email addresses.
Introducing Cyber Advisors - https://iasme.co.uk/articles/introducing-cyber- advisors/
Introducing Cyber Advisors - https://www.ncsc.gov.uk/schemes/cyber- advisor Become a Cyber Advisor - https://thecyberscheme.org/cyber-advisor/ What will Cyber Advisors do and how much will they charge? - https://iasme.co.uk/articles/what- will-a-cyber-advisor-do-and-how-much-will- they-charge/
What are the benefits, requirements, and costs of becoming a Cyber Advisor assured service provider? - https://iasme.co.uk/articles/what-are-the-benefits- requirements-and-costs-to- becoming-a-cyber-advisor-assured-service-provider/ What is the purpose of the Cyber Advisor scheme? - https://iasme.co.uk/articles/what-is-the- purpose-of-the-cyber-advisor- scheme/
What is the difference between a Cyber Essential certification body and a Cyber Advisor assured service provider? - https://iasme.co.uk/articles/what-is-the- difference-between-a-cyber- essentials-certification-body-and-a-cyber-advisor- assured-service-provider/

You can also email:
info@iasme.co.uk with general questions about the scheme.
info@thecyberscheme.org for information about assessment centres.

Version control

Date	Version Number	Changes	Author
8th February 2024	1.0	First issue of document	Peter Loomes
9th February 2024	1.1	Corrections after internal QA	Peter Loomes
4th June 2024	1.2	Update to marking criteria and rewording of Cyber Advisor and Assured Service Provider criteria and eligibility	Sharon Reece