# Cyber Advisor Assessment

## GUIDANCE FOR CANDIDATES

THE IASME CONSORTIUM | WYCHE INNOVATION CENTRE, MALVERN

## 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 the 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 cyber security 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, cyber security, and providing consultancy to different types and sizes of business.

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.

# Practising 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 cyber security 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 steps:

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:
   a. UKAS accredited ISO 27001* certification or
   b. IASME Cyber Assurance Levels 1 and 2
6. Meet requirements demonstrating good quality standards. This can be achieved by holding **one** of the following quality certifications:
   a. UKAS accredited ISO 9001* certification or
   b. QG Quality Fundamentals+ certification or IASME Quality Principles (achieved and audited as part of IASME Cyber Assurance Level 2 certification)
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. The Knowledge, Skills, and Behaviours are taken from the NCSC Cyber Advisor Scheme Standard https://www.ncsc.gov.uk/files/NCSC-Cyber-Advisor-Standard-v1-1.pdf

## Duties (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 the appropriate and proportionate actions to address the 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 Advisor 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-it-infrastructure-v3-2.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 Get Ready for Cyber Essential 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 do it, or 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 cyber security 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 | Determine suitable and proportionate mitigation strategies 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 | | Explanation |
|---|---|---|
| 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/ethical-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 not a typical cyber security exam. It is designed to test both the candidate's knowledge of cyber security and the way they interact with and provide advice to clients.  The assessment is designed to mimic a client engagement as follows:

## Timings

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

Candidates will be presented with real-life business scenarios. There will be one scenario for each assessment centre and all parts of the assessment will centre on that scenario.

Candidates 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;
- Collaborate with customers or their representatives;
- Implement solutions.

Throughout the process, assessors will observe candidates against the knowledge skills and behaviours previous discussed on page Duties, Knowledge, Skills, and Behaviours of a Cyber Advisor5, and will note candidates' responses to the requirements of the assessment.

# The two parts of the assessment

## 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 to complete this part of the assessment.

This part of the assessment includes 12 multiple-choice questions and 12 short-form written answers. Candidates have two hours to answer the questions[1]. The questions are based on a real-life business scenario, and candidates are encouraged to read the short-form questions carefully as they will expand on the multiple choice and will definitely require additional content.

This part of the assessment evaluates:

1. The candidates' understanding of the Cyber Essentials' requirements
2. The application of the controls at an appropriate level for the business, based on its size, complexity, budget, and plans
3. Use of reference sources
4. 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.

# Using refences in the assessment

The assessment is open book, and candidates can either bring reference material with them, or access information from the internet during the assessment. If references are used, candidates are required to quote their sources in any answers they provide.

[1] Candidates who normally have extra time in assessments can request this at the time of booking.

# Example scenario, question and model answer

## Scenario[i]

MotorMouth (see footnote 1) Ltd are a small public relations company. They are planning to work with an NHS Trust to manage some external communications. The NHS Trust require MotorMouth to obtain Cyber Essentials before they commence working with them.

MotorMouth is owned by Virginia Manga, she has two other staff:

- Jill Bott is Virginia's assistant and manages her own client caseload
- William Willing is an apprentice, he does not have a caseload at the moment but supports both Virginia and Jill with their work. As the youngest and most technically knowledgeable person in the business, William manages the IT

The technical environment

- 2 Apple MacBook Pros both 2024 models with M3 Processors running MacOS 15
- 1 Mac mini 2020 model running MacOS 14
- 1 iPhone 15 running iOS 18
- 1 iPhone 13 running iOS 18
- 2 iPad airs running iPadOS 18
- 1 TP-Link Archer AX10 Router
- 1 HP Officejet 8122e Printer

William does not have a company mobile phone but uses his personal mobile to access Microsoft Teams and Outlook. This phone is a Samsung Galaxy Z Flip.

MotorMouth use the following applications:

- Microsoft 365 Office Business Standard (all three staff)
- Xero accounts (one account only used by Virginia)
- Adobe Creative Cloud (all three staff)

## Part one of the assessment

### A sample multiple choice question

In relation to this scenario, one multiple choice question may be:

Q. When setting up a new computer for the business, which of the following actions should they implement to be compliant with Cyber Essentials?

A. Enter the details of the router into the asset register
B. Remove all unused and unnecessary software
C. Connect the device to the internet as soon as possible
D. Check that it will run the applications the business wants to use

The only answer here that is discussed in the Cyber Essentials Requirements is B. So, B would be the correct answer.

## A sample shortform question

William has read the Requirements for IT Infrastructure Document and knows that he needs to remove any software the business does not use. He asks how he can establish what is and isn't needed.

A reasonable approach would be to write an email to William which could read as follows:

*Dear William*

*I appreciate that it can be difficult to know what software is used and what isn't. However, it is important to remove software that is not used, because this may not be updated and therefore, may introduce vulnerabilities to your environment.*

*My first recommendation would be to discuss with each of the users what they use their computers, phones and tablets for, and how your environment supports this activity. You could develop a grid of the software you have installed and map the activities to the installed software. When you have completed this exercise, you will be able to see where you have applications that are not being used.*

*For example, I note that you are using MS365 for your word processing, presentation, spreadsheets and communications. On your Macs there are applications that duplicate this activity, such as: Pages, MacMail, Sheets, and Keynote. I suspect you will find these are not used and can be removed.*

*It will be a good idea to document what applications each of you use, and therefore need installed on your devices, so if you ever need to rebuild a device because of an issue, you know exactly what to install and remove. If you want to come up with an initial list for each device you have, I would be happy to help you review it.*

*Kindest regards*
*Annette Curtain*
*Cyber Advisor*

In this response Annette has explained in simple terms why removal of software is required and has suggested a relatively simple way of identifying what is and what is not needed. This is a three-person company, so it is realistic to do this manually. Annette has also suggested that not only should they remove the applications, but they should record what the standard build is for each device, as this could come in useful later. She has also recommended some applications which may not be required.

Finally, Annette has offered further assistance if it is needed.

In part one of the assessment, there will be 12 multiple choice questions and 12 related shortform questions. However, be aware that you may be tested outside of the scope of Cyber Essentials, such as other NCSC guidance or relevant standards. For example, you may have a multiple-choice question that asks:

*What is the minimum password length for passwords in Cyber Essentials?*

This may be followed up by a short form questions that asks:

*William has noted that it is good practice to have a password policy, and has asked you if you could recommend what should be included in the policy, how would you respond?*

Resist just referring William to the NCSC password guidelines. What the assessment process is looking for is the candidate to understand the requirements and present those requirements to the customer at a level that is appropriate to the size of the business. In this case, it is a very small business and processes can be quite simple.

## Part two of the assessment

This is a discussion, not an interview. The idea of the discussion is to mimic a customer engagement, where a customer may ask the consultant to clarify recommendations they have made.

Whilst the candidate is completing the shortform and multiple-choice questions, the assessor will look at the answers they are providing. The assessor will choose between five and seven areas from the answers provided by the candidate to explore further. It is difficult to give examples of these types of questions as they are specific to the candidate. However, the candidate should answer them as though they are talking to their customer, they should not assume any knowledge on the part of the assessor.

# How the assessment is marked

## Multiple Choice

This is marked automatically in the assessment platform, there is only one correct answer per question.

# Short form and discussion

The short form and discussion are marked in the same way, and the overall marks are combined to get a final mark, this will be discussed 14later . The assessors are looking for candidates to provide the following in their answers:

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 marks the answers provided as either: Insufficient, below expectations, meets expectations, or comprehensive. The platform then assigns the appropriate mark for the description, as shown in the table below:

| Assessor Score | Made up from | System 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 |

# Passing the assessment

## Multiple-choice

The candidates must achieve a mark of 80% or higher to pass the multiple-choice section of the assessment. If the candidate fails the multiple-choice section of the assessment, they will fail the assessment outright.

## Shortform and discussion

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 us 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 marks for the shortform and discussion are added together and then averaged to give an overall score for the two activities, this average score must be 75% or above for the candidate to pass.

The following tables demonstrate how the marking for the shortform and discussion work.

Table 1

| | 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 |
| | | |

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.

Table 2

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

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.

To recap, to pass the assessment a candidate must attain a mark of 80% or more in the multiple-choice section and a combined score of at least 75% in the shortform and discussion sections.

# 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 “ found in the Cyber Essentials technical section of the NCSC website https://www.ncsc.gov.uk/cyberessentials/resources
- 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 advisable 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 Open Worldwide Application Security Project (OWASP), or SANS Institute 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 that they have 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 is 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 NCSC, IASME and The Cyber Scheme websites and search for Cyber Advisor.

Candidates can also email questions to:

- info@iasme.co.uk with general questions about the scheme
- info@thecyberscheme.org for information about assessment centres

| 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 |
| 20th January 2025 | 2.0 | Updated with details of the marking scheme and a new sample question. | Peter Loomes |
| 27th January 2025 | 2.1 | Updated after comments from the quality assurance process. | Peter Loomes |

[i] Any resemblance in this scenario either currently in existence or previously operating is pure coincidence. Any references to people are also fictitious and any resemblance to anyone living or dead is coincidence.