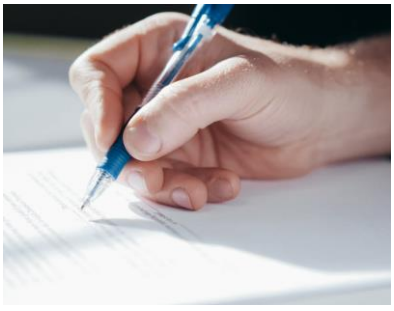
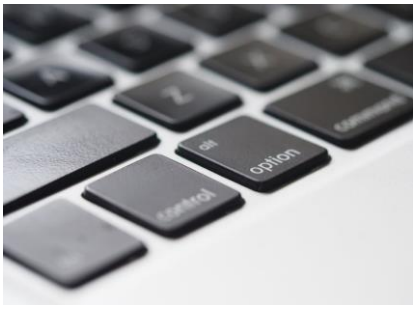




NCSC Cyber Advisor (Cyber Essentials): Guidance for applicants

Contents

Document Control

Version ID

Version 1.0

Version Control

Date	Version	Change
15 August 2022	1.0	First version of the document

Related Documents

- IASME Consortium – NCSC the Advisor, Code of Conduct.
- Duties, Knowledge, Skills, behaviours and Assessment Criteria Library – Document ID CE28012022-2
- NCSC Cyber Essentials: Requirements for IT Infrastructure document. Version 3 November 2021

Distribution

No restrictions

Introduction

The Cyber Advisor (Cyber Essentials) assessment and certification assures businesses that the holder is competent to advise on and implement the requirements of the Cyber Essentials scheme and the value of certification.

The National Cyber Security Centre (NCSC) is nationally recognised as the technical authority for cyber in the UK. This certification is endorsed by the NCSC and is managed to their high standards. Businesses considering implementing Cyber Essentials can therefore have assurance that holders of the certificate:

- are competent
- comply with standards and a code of conduct
- have a focus on customer service.

Duties of the Advisor

The Advisor is expected to be able to carry out several duties, these are:

- Conduct a Cyber Essentials gap analysis.
- Develop and present reports on the status of Cyber Essentials controls.
- Agree on remediation activities for Cyber Essentials controls.
- Plan remediation activities sympathetically to operations activities.
- Implement remediation activities sympathetically to operational activity.
- Develop and present post-remediation/engagement reports.

Cyber Advisors practicing as part of a Certified Advisor Service will be required to sign and work to a code of conduct. In order to carry out these duties, Advisors will be required to demonstrate relevant knowledge, skills and behaviours during the assessment process.

Assessment process, preparation and rules

Prepare for the assessment

All applicants are responsible for ensuring they are ready for the assessment. In preparation, applicants should understand:

- The duties, knowledge, skills, behaviours and assessment criteria required of the Advisor; details can be found in the Cyber Advisor Scheme Standard at https://www.ncsc.gov.uk/files/Cyber-Advisor-Scheme-Standard.pdf. Prospective applicants should self-assess against these requirements and only book the assessment once they meet them.
- Understand the NCSC Cyber Essentials: Requirements for IT Infrastructure Document found at https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf. This document is the authoritative guide to the requirements for Cyber Essentials.

Booking the assessment and fees

Due to this being a Proof of Concept (PoC) the assessment costs are free (funded by NCSC) for the first 100 applicants; future cost of the Cyber Advisor Exam will be £550. Noting that to operate as a registered Cyber Advisor there will be an annual charge per individual Advisor (£250) and per NCSC Assured Service Provider (£600). In addition, there is an onboarding fee of £250 for each new Advisor.

Applicants requiring reasonable adjustments must inform the assessment body at the time of booking. Applicants may be asked to consider alternative assessment dates to ensure the reasonable adjustments can be implemented appropriately.

Assessment

The objective of the assessment is to ensure that applicants have the necessary competence to perform the duties of the Advisor.

The applicant will be presented with real-life scenarios and will be required to understand the organisation and any issues they may have in achieving compliance with the Cyber Essentials controls. During the assessment, the applicant 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 applicants; Assessors will note the applicant's responses to the requirements. To ensure fairness of the assessment, Assessors will be provided with reference material to assess against.

The assessments will typically take 2-3 hours.

Before the assessment

It is the applicant's responsibility to arrive in time for the assessment. Applicants will need to confirm if any reasonable adjustment is required before the assessment.

On the day

Applicants are required to arrive at least 30 minutes before the assessment starts. Applicants who arrive late may not be allowed to participate and will forfeit the assessment fees.

If an applicant is delayed in arriving at the assessment centre, they must contact the assessment centre staff as soon as possible.

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

- UK photo driving licence
- passport
- government issued photo ID
- photo ID issued by an employer

The applicant will not be able to take anything into the assessment. All materials required during the assessment will be provided.

The assessment will be open book, though there will be a requirement for all applicants to record all URLs used for reference e.g. configuration data for vendors.

Receiving the results

Applicants will receive their results within one month of the assessment taking place, this is due to this being a PoC and moderation of results is required at the end of each cohort of assessments. There will be an opportunity for successful applicants to receive feedback on aspects of the

knowledge, skills, and behaviours that could be improved. Unsuccessful applicants will be offered feedback on areas to concentrate on before the next assessment. The results of the assessment will only be provided on the proviso that the mandated PoC feedback form is completed, as this will help define the potential Cyber Advisor scheme that may follow from the PoC.

Certificates

Certificates will be issued by the assessment body to successful applicants within one working week of the results being disclosed. The certificate is only proof of passing the Cyber Advisor assessment. To be eligible to offer Cyber Advisor services under the scheme organisations will need to become an Assured Service Provider registered with IASME and employ at least one formally assessed Cyber Advisor.

Retaking the test

Unsuccessful applicants wishing to retake the test will be required to wait before resitting. The time will be based on their overall scores as follows:

- Within 10% of the pass mark - resit four weeks after the original exam.
- Within 20% of the pass mark - resit six weeks after the original exam.
- More than 20% off a pass mark - resit eight weeks after the original exam.

Applicants that fail the assessment three times will be required to wait a minimum of four months before resitting the assessment. This is to ensure that the applicant has had time to prepare fully using the feedback provided during previous assessments.

For all resits, applicants will be required to cover the assessment costs.

Registering as an Advisor

In the event that the successful applicant wishes to become an approved Cyber Advisor (Cyber Essentials), they will need to register with the IASME Consortium before the expiry of their certification.

Securing the assessment content

Professional certifications are essential in assuring the expanding area of cyber security. To maintain a fair and balanced assessment, the security and confidentiality of the assessment content have to be assured. The Cyber Scheme (https://thecyberscheme.org/) has taken steps to reduce the possibility of cheating or gaming in the assessments; however, we still rely upon the ethical behaviour of professionals who have undergone an assessment to support the protection and privacy of the content. Applicants who undertake the assessment will be bound by The Cyber Scheme terms and conditions and any disclosure of information about the content of assessment centres will be considered in direct violation of those terms. The IASME Consortium (https://iasme.co.uk/) will act against individuals who violate such rules and policies, including permanent revocation of their Advisor certification.

Appealing the assessment decision

All applicants have the right to appeal the decision of the Assessor. In the first instance, they should contact The Cyber Scheme at https://thecyberscheme.org/contact/

Appendix A – example scenario

Scenarios are designed to reflect a typical consulting assignment. The applicant will initially be presented with background information about a business which they will need to evaluate and react to, as they would when working within a company.

StayUp is a small building contractor; they are subcontractors to a larger building company that has just won a contract to build an annexe to a secondary school. The Local Education Authority (LEA) insist that the prime contractor certifies to Cyber Essentials at the self-assessed level as a minimum. The prime contractor has included this requirement in all their subcontractor agreements.

About the business

StayUp employs 30 people as follows:

- Nia is the Managing Director and owner of the business. Her responsibilities include:
  - quoting for work
  - project managing the delivery of work
  - managing the office
- Richard does general administration finance and manages IT
- Kathy is part-time and manages HR and payroll
- Greg is an apprentice and works with Richard doing general admin and IT support
- The other team members are what Nia refers to as the trades

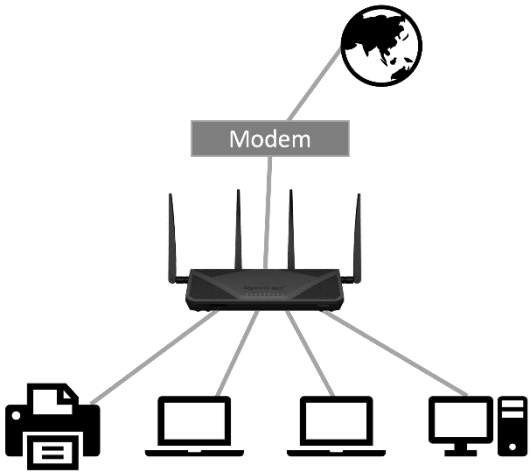
The IT

Hardware

The IT is not complicated and is made up of the following:

- 1 X Dell Latitude 5450 running Windows 8.1 Pro 64bit
- 2 X Dell Inspiron 15 3000 running Windows 11 Home
- 1 X HP Elite 8300 SFF running Windows 10 Pro
- 1 X Synology RT2600 ac Router
- 1 X DrayTek 130 Ethernet Modem
- 1 X HP OfficeJet Pro 7740

Network



Working arrangements

- Richard and Greg are fully office based with no remote working.
- Nia occasionally works from home, where she connects her business laptop to the internet through her home ISP supplied router. When on customer sites, if she connects to the internet, it will usually be via the customer's network.
- Kathy works two days from home and one day in the office. When at home, Kathy connects her business laptop to the internet using her home ISP supplied router.
- The trades work mainly on customer sites and have no access to any business IT.

Applications and business services

StayUp uses the following applications and business services:

- Google Workspace for:
    - file storage
    - email
    - word processing
    - spreadsheets
- QuickBooks accounting
- Zoho People HR and Payroll

The Advisor can then expect to be asked questions such as:

- What would be in the scope of Cyber Essentials?
- What issues do you see with the IT environment regarding Cyber Essentials?
- Demonstrate how you would check the configuration of the primary boundary firewall.

The course of the assessment conversation will be based on the answers to the initial questions as the assessor probes the depth and breadth of the applicant's understanding.