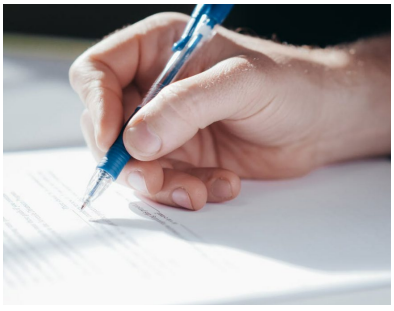

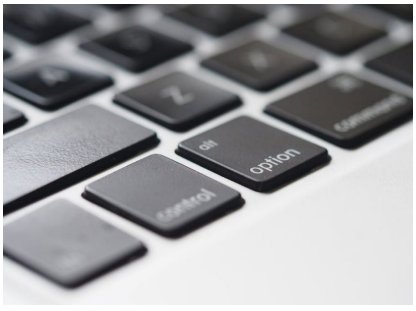

NCSC Cyber Advisor Scheme: Standard

v1.1

Contents

Background context

Cyber Essentials is a certification scheme set up by government, and run by The IASME Consortium[1] on behalf of the NCSC, to help organisations protect themselves from common cyber attacks. There are two levels of certification: Cyber Essentials, which is based on a verified self-assessment; and Cyber Essentials Plus, in which independent technical verification of the controls is undertaken. Currently, more than 100,000 Cyber Essentials certificates have been issued to organisations.

It is now becoming apparent that there are a large number of micro businesses as well as small and medium-sized enterprises (SMEs) across the UK that would like to acquire the protection that the Cyber Essentials controls provide but who do not have the internal resources or skills required to perform the gap analysis or implement the required controls.

Cyber Advisor scheme

To address this need, the National Cyber Security Centre (NCSC) is piloting a scheme to certify Cyber Advisors (Cyber Essentials). The duties of Cyber Advisors include working with organisations that would like to strengthen their defences against cyber attacks, carrying out gap analyses, and implementing the required controls.

It is anticipated that the benefits of the Cyber Advisors scheme would include improved cyber resilience across UK SMEs and micro businesses – especially those currently unsure about how to access good quality cyber security support to implement a minimum baseline of cyber security. Increased take up of Cyber Essentials may be an additional benefit of the service.

Overall approach to the certification of Cyber Advisors

The Cyber Advisor scheme identifies:

- The duties that Cyber Advisors would be required to undertake.
- The knowledge, skills[2] and behaviours required by Cyber Advisors to successfully carry out their duties.
- A set of assessments that applicants for Cyber Advisor would need to undertake – the assessments cover all the duties that Cyber Advisors would be required to carry out.

Duties of Cyber Advisor (Cyber Essentials)

This list shows a Cyber Advisor's duties:

D1. Conduct Cyber Essentials gap analysis.
D2. Develop and present reports on the status of Cyber Essentials controls.
D3. Agree remediation activities for Cyber Essentials controls.
D4. Plan remediation activities sympathetically to operations activities.
D5. Implement remediation activities sympathetically to operational activity.
D6. Develop and present post-remediation / engagement reports.

[1] https://iasme.co.uk/cyber-essentials/

[2] https://www.open.edu/openlearn/mod/oucontent/view.php?id=20017&section=1 has a useful discussion of the difference between knowledge and skills: knowledge is information, facts or understanding about a domain; a skill is concerned with the ability carry out a task or apply knowledge.

Knowledge Areas

Cyber Advisors will need to have a good understanding of the Knowledge Areas, shown in the following list:

K1. Detailed understanding of the latest version of the NCSC Cyber Essentials Requirements for IT Infrastructure.
K2. An understanding of the NCSC Small Business Guide: Cyber Security.
K3. An understanding of the NCSC Cloud Security Guidance.
K4. Understand the basis of common threats and how they apply to businesses they are dealing with.
K5. An understanding of secure home and remote working approaches.
K6. An understanding of secure development industry good practice guidance.
K7. Knowledge of gap analysis frameworks to help organise work.
K8. Knowledge of current Cyber Essentials appropriate technical controls approaches.
K9. Understanding of dependencies between each of the Cyber Essentials controls.
K10. Implementing current Cyber Essentials controls.
K11. Information sources relevant to the implementation of Cyber Essentials controls.
K12. Understanding business and technical dependencies relevant to the implementation Cyber Essentials controls.

Skills

The skills that Cyber Advisors will need to apply in their duties are shown in the following list:

S1. Organisation and planning.
S2. Negotiation.
S3. Communication.
S4. Investigation / Audit.
S5. Ability to explain technical requirements in non-technical business language.
S6. Record Keeping.
S7. Ability to identify appropriate and proportionate approaches for a business to mitigate the identified gaps in the Cyber Essentials requirements.
S8. Report writing.
S9. Presentation.
S10. Ability to understand business priorities of clients.

Behaviours

The behaviours that Cyber Advisors would be expected to display whilst undertaking their duties are shown in the list below:

B1. Professional approach.
B2. Collaborative approach.
B3. Non-judgemental.

Mapping of knowledge, skills and behaviours to Cyber Advisor's duties

For each duty required of a Cyber Advisor, the full documentation set identifies the knowledge, skills and behaviours required for a Cyber Advisor to successfully carry out that duty.

Assessment of applicants for certification as a Cyber Advisor

The assessment criteria against which applicants will be assessed are shown in the list below. The criteria ensure that all of the knowledge areas, skills and behaviours listed in the previous sections are covered.

A1. Ability to understand the NCSC Requirements for IT Infrastructure Document (RITID) and CE Question Set.
A2. Ability to apply RITID to a business scenario.
A3. Ability to define a realistic CE assessment scope for a defined business scenario.
A4. Ability to align the CE requirements with other NCSC guidance.
A5. Ability to align CE requirements with industry good practice and guidelines such as M365 Security, AWS Security, Azure Security, SANS, OWASP etc.
A6. Ability to gather appropriate evidence to make measured judgements.
A7. Ability to assimilate evidence into logical conclusions for reporting.
A8. Constructing a report on findings using the appropriate language for the target audience.
A9. Knowledge of reliable sources of reference materials for Threats.
A10. Knowledge of reliable reference sources for implementation of CE controls.
A11. Ability to construct a plan of action considering organisational pressures.
A12. Ability to negotiate with clients, client-side staff and third parties to schedule remediation activities.
A13. Ability to construct a plan of action considering technical dependencies.
A14. Ability to present the plan of action to the business using language appropriate to the audience.
A15. Ability to implement controls and configure IT equipment to meet the requirements of the RITID (active version).
A16. Ability to implement controls in a manner sympathetic to the business operations.
A17. Ability to record details of implementation activities and configuration of IT components following organisational processes and language appropriate to the business.
A18. Ability to be able to present findings to an audience using appropriate language.

The full document set shows for each duty the relevant assessments, knowledge areas, skills and behaviours.

How assessments will be carried out

All applicants are responsible for ensuring they are ready for the assessment. In preparation, applicants should have a good understanding of:

- The duties, knowledge, skills and behaviours required of a Cyber Advisor as well as the Assessment Criteria – details about the Cyber Advisor assessment can be found on the Cyber Scheme website at https://thecyberscheme.org. Prospective applicants are advised to self-assess against these requirements and only book an assessment once they consider they meet the requirements.
- The NCSC Cyber Essentials Requirements for IT Infrastructure, which can be downloaded from https://www.ncsc.gov.uk/cyberessentials/resources.

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.

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 Cyber Essentials controls. During the assessment, applicants 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 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.

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

Applicants will not be able to take any materials into the assessment with them. 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.

How to apply

Applications to become a Cyber Advisor should be submitted using the appropriate form on the IASME website. All applications will be received and dealt with by the Cyber Advisor delivery partner, IASME.