Cyber Essentials Service Description

Version 2.0

claranet

Make
modern
happen®

Contents

1. What is Cyber Essentials?

Cyber Essentials is a UK government-backed certification scheme that helps organisations protect themselves against common cyber threats. The scheme provides requirements and guidelines on a set of basic security controls that all organisations can implement to reduce the risk of cyber-attacks through.

The scheme is designed to be accessible and affordable for organisations of all sizes. It provides two levels of certification:

Cyber Essentials Verified Self-assessment:

The self-assessment process involves an organization evaluating their cybersecurity posture against five fundamental security controls. This self-assessment is then reviewed and verified by an independent qualified Cyber Essentials assessor who is associated with a Certification Body.

Cyber Essentials Plus:

Cyber Essentials Plus is a technical verification of the same five security controls by a Cyber Essentials Plus assessor. It involves a hands-on approach to validate the self-assessment previously completed, through a series of physical tests, including a vulnerability assessment.

The scheme provides requirements and guidelines around five technical control themes:

Firewalls

Secure Configuration

Access Control

Malware Protection

Patch Management

And also highlights the importance of:

- **Asset management, Vulnerability assessment and Policy and Procedure**

To achieve Cyber Essentials certification, organisations must complete a self-assessment questionnaire and have their responses independently verified by a certification body. Claranet Cyber Security is a licensed IASME certification body (CB) to certify any size organisation against Cyber Essentials Verified Self-assessment and plus.

2. Benefits of Certification

The Cyber Essentials scheme provides several benefits for organisations, including:

1. **Improved cybersecurity:** The scheme helps organisations implement basic controls to protect against common cyber threats.

2. **Exposure to industry-leading Controls:** The standard provides guidelines on industry best practices for cyber security.

3. **Competitive advantage:** Cyber Essentials certification can help organisations stand out from competitors and win new business.

4. **Compliance:** The scheme can help organisations demonstrate compliance with relevant regulations and standards.

5. **Peace of mind**: Cyber Essentials certification provides peace of mind that the organisation is taking cybersecurity seriously.

3. Cyber Essentials Verified Self-assessment

The Cyber Essentials self-assessment service is facilitated through an online portal and covers five essential areas of cybersecurity. Clients are required to submit self-assessment questions, which are then reviewed, discussed, and audited by qualified Cyber Essentials assessors during a dedicated Marking session.

To initiate the process, the Client must first have an initial discussion with a Claranet sales account management team. Following this, the Client is required to complete and submit an online account creation form, which serves as the input to activate the processes described above.

3.1. Process Overview

1. To initiate the Cyber Essentials certification process, you will need to provide Claranet Cyber Security with a Purchase Order. Once confirmed, you will receive details of the scheduled assessment marking date, along with a link to an online information form for Cyber Essentials.

2. To proceed further, you will need to complete and submit an online account creation form which will be provided by Claranet. Claranet will create your account in the Cyber Essentials Portal (CE Portal), and you will receive an email with a link to your self-assessment questionnaire.

3. You will receive temporary login credentials via SMS, which you will need to change before proceeding to complete the self-assessment questionnaire.

4. You will begin to populate your answers to 70+ questions in the assessment portal.

5. During this time, you can discuss your self-assessment questionnaire responses with your Claranet Assessor, who will offer guidance were required.

6. Once the assessment has been populated with your initial answers the Claranet Assessor will pre-check your assessment and provide an interim report of the findings. In the event the assessment is not compliant you will be offered a maximum of 30 days to remediate non-conformities. Claranet will provide a second pre-check, further remediation or checks are offered at the discretion of Claranet and may incur additional costs.

7. Once you and the Claranet Assessor are satisfied that the responses accurately reflect your organisation's adherence to the requirements, you will be asked to submit the response in the CE Portal

8. You will then receive an automated email confirming the submission of the self-assessment questionnaire.

9. Your self-assessment questionnaire responses will be officially scored, and you will receive a notification of the result via an automated email.

10. If your responses are insufficient to achieve a Cyber Essentials pass, a report will be generated and sent to you, along with commentary from the Claranet Assessor, to help guide your remediation activities to try and gain a pass.

11. If the self-assessment questionnaire responses are sufficient to achieve a pass, you will be sent confirmation of certification status.

12. The Claranet Assessor will provide support in managing your certificates through Blockmark which is a digital system for managing IASME-related certificates.

3.2. Responsibility Model

Responsibility	Claranet	Client
Quotation: Provide a high-level quotation containing the cost of Cyber Essentials and/or Cyber Essentials Plus engagement. This is a Sales Order Form for signature.	✓	
Purchase Order: Provide a Purchase Order reference for invoicing, alongside a signed copy of the Sales Order Form. This must happen before any dates can be agreed upon and before a CE Portal account can be created.		✓
Portal Account: A link to an account creation form will be sent to the Client for completion so that an account in the CE Portal can be set up.	✓	
Portal Account Activation: A link to the Client account is sent via email, and temporary access credentials are sent via SMS to a nominated mobile		✓

device. To activate the account, change the password within the CE Portal within 48 hours.		
Completing the Questionnaire: The client can begin completing the self-assessment questionnaire. This **must** be completed within 6 months. Once completed, SAVE (**DO NOT SUBMIT**) the self-assessment questionnaire until during your designated Marking Period.		✓
Marking Period: There may be contact throughout the Marking Period to discuss the self-assessment questionnaire responses, validate the answers provided and provide guidance on how best to approach questions.	✓	
Submitting Questionnaire: The Client shall submit the self-assessment questionnaire in the CE Portal for formal scoring before the conclusion of the Marking Period.		✓
Remediation: In the event of non-compliance after the pre-check, the Client shall be informed of any remediation required. This must be achieved, and a successful passing submission be completed within 3 days of the initial marking.		✓
Results: Once submitted and scored, the results will be sent to you. This will be either a report showing where the questionnaire failed to reach the required standard or a confirmation of a pass.	✓	

4. Cyber Essentials Plus

After achieving a PASS for Cyber Essentials certification, the organisation can proceed to achieve certification for Cyber Essentials Plus by undergoing a Technical Audit of their organisation based on the scope of their Cyber Essentials submission.

Cyber Essentials Plus certification is awarded to an organisation after a Technical Audit has been conducted, which includes:

- External and internal vulnerability scan of end-user devices, servers, and infrastructure
- Various tests against the five key technical controls to confirm Multi-Factor Authentication (MFA) in cloud environments, to confirm account separation between Users and Administrators, to confirm anti-malware defences for browsers and email clients, to confirm the ability to install unsigned applications
- Depending on your listed controls a CE+ audit may also include an MDM review

To achieve Cyber Essentials Plus certification, the Technical Audit and report must be completed and submitted to IASME no later than three months following the award of Cyber Essentials certification.

4.1. Process Overview

The first stage of the Cyber Essentials Plus certification process is Scoping, which involves identifying the scope of the assessment. Once this has been completed, the Client can proceed with the following steps:

1. Confirm their wish to proceed by sending a Purchase Order and signing the Sales Order Form (unless this has already been completed).
2. Agree on dates for Technical Audit Days with Claranet.
3. This process description continues at the point where Cyber Essentials Self-Assessment has been achieved.
4. The Cyber Essentials Plus Technical Audit Days usually take place a minimum of two weeks after passing the Cyber Essentials certification to allow for self-assessment remediation and vulnerability scanning to be completed. In the event of a large scope that may require more time, this will be identified during scoping, if urgent deadlines are requested this can be shortened if applicable.
5. The Cyber Essentials Plus audit can be delivered remotely or on-site and includes a physical assessment of end-user devices and mobile phones. Externally facing infrastructure is subject to a vulnerability scan and manual brute force assessment where authentication is required.
6. Testing of a sample of devices is carried out by the Claranet Assessor within the boundary of the scope and can include end-user devices that connect to the Clients organisational data and services, servers upon which standard users obtain an interactive desktop, servers that are internet-connected and all types of cloud services (IaaS, PaaS, SaaS) are subject to specific test’s. The Claranet Assessor shall advise the Client, as appropriate, of sample sizes required before the Technical Audit.
7. A Reporting Day takes place immediately after the Technical Audit Day(s). Claranet shall document the results of their audit and highlight any non-compliance results.
8. An the event of non-compliance, the Client has 30 days to complete any remediation actions from the last date of their Technical Days. A date will be set for remediation to be completed by. Following any non-compliance and Client remediation, Claranet shall retest to confirm compliance.
9. Submission is scored, and the Client is provided with confirmation of pass or fail. The Client will be notified of a pass or fail.

4.2. Responsibility Model

Responsibility	Claranet	Client
Complete Scope Form: Provide the information required on the online scope form. This is used to determine how many days are required for the Technical Audit and the length of time vulnerability scans will need to be complete.		✓
Quotation: Claranet shall provide the Client with a quotation for Cyber Essentials Plus based upon the scoping information provided.	✓	
Purchase order: Client provides Purchase Order reference for invoicing, alongside a signed copy of the Sales Order Form. This is required before dates for Technical Audit Days can be agreed upon and confirmed and before your account in the CE Portal can be created.		✓
Completion of Cyber Essentials: Client is responsible for ensuring Cyber Essentials is completed and successfully passed prior to the scheduled Technical Audit Days.		✓
Technical Audit Readiness Call: Claranet Assessor will arrange a technical audit reediness call with Client, to discuss the logistics of the audit including selecting a suitable device sample and to discuss the external scan.	✓	✓
External Scan Setup: Claranet Assessor will configure the external scan prior to the Technical Audit Days and communicate this with Client.	✓	
Technical Audit Days: A Claranet Assessor will deliver a remote or optionally onsite Technical Audit against the Cyber Essentials Plus test specification and discuss the results of external vulnerability scans. Typically, Technical Audits take place over 3 to 4 days.	✓	
Reporting Day: Typically takes place immediately following the conclusion of Technical Audit Days. The Claranet Assessor analyses the results of the Technical Audit and, using the portal, writes a report which will lead to a pass/fail notification.	✓	
Remediation: The client has a maximum of 30 days to complete any remediation work. Dates for remediation shall be agreed upon with the Claranet Assessor to ensure enough time is available to retest.		✓

Notification of Result: The client will receive notification of the result alongside a report.	✓	

5. Cancellations and Delays

Claranet Cyber Security will assign a Cyber Essentials Assessor to your service based on the agreed dates and the availability of an appropriate assessor. If there is a delay or cancellation before or during the test, the appropriate fee will be payable. Further details can be found in the Appendix A.

6. Communication

Efficient engagement requires clear lines of communication, which cover timely transfer of information, how it is achieved, frequency, and personnel involved. Providing the requested information as quickly as possible, using online forms and self-assessment questionnaires provided, enables Claranet to respond promptly and keep Clients updated.

6.1. Responsibility Model

Responsibility	Claranet	Client
Claranet Contact information: Provide details of the Claranet Assessor delivering service.	✓	
Audit Contacts: Provides contact details of Client staff Claranet are to deal with during Assessor Days and Technical Audit Days.		✓
Update frequency: The client receives email confirmations each time an account creation form, scope form, or self-assessment questionnaire is submitted. The Client receives via email and text message login details for the CE Portal account. Notification of PASS or FAIL is delivered via email alongside any reports.	✓	
Scheduling: Inform Claranet of any changes to required dates or contact details as early as possible. Changes to dates may result in additional costs.		✓
Scheduling: Inform you promptly of any necessary changes to dates or the Claranet Assessors involved in the delivery of the engagement.	✓	

7. Handling of Sensitive Data

To protect any sensitive data or information encountered during the engagement, Claranet Assessor machines are encrypted. Regular scrubbing of devices ensures that data is not retained. All Cyber Essentials assessment/audit data will be sent encrypted either using AES-256 password-based encryption or using a secure portal that the client provides.

7.1. Responsibility Model

Responsibility	Claranet	Client
Sensitive data: Act per the Claranet Cyber Security practice for the handling of your sensitive data and general best business practice. Claranet Assessors will, where possible, avoid coming into the possession of Personally Identifiable Information.	✓	

8. Appendix: A

8.1. Terminology

Throughout the document or in association with it, several terms have been used. These can be found in the general description below.

CB	Certification Body
Certification Body;	Licenced organisation who can deliver Cyber Essentials Certification to business, governed by the NCSC and IASME
Claranet Assessor	an IASME trained and qualified Cyber Essentials assessor employed by Claranet Cyber Security.
CE Portal	Cyber Essentials online assessment Portal
Marking Period	the time assigned to clients to audit questionnaire responses, deliver remote technical audits, produce CE+ reports as well as provide consultancy and advice on cyber security best practices.
Master Services Agreement (MSA)	This is a legal document provided by Claranet to the client which sets out and explains the legal conditions of the sale.
Personally Identifiable Information (PII)	Technical contact name, email address and phone number
PO	Purchase order
Report Day	A period of time towards the end of the audit for the assessor to compile and complete the Cyber Essentials report.
Sales Order Form	• document containing pricing and other details of the service being purchased. The signing of this quotation document by the client

	confirms the purchase contract between both parties.
Statement of Work (SoW)	Document completed by Claranet and provided to the client at the conclusion of the scope stage, which confirms the scope of the engagement and the activities that will take place during the engagement.
Technical Audit	Cyber Essentials Plus audit to validate adherence to the Cyber Essentials test cases against a pre-agreed sample of devices
Technical Audit Days	the time set aside to audit the Client organisation based on the scope of their completed Cyber Essentials Self-Assessment Questionnaire.

8.2. Cancellations and delay charges

Cancellation timescale	Cancellation fee (% of engagement price)
Cancellation request received more than 30 working days prior to start date.	25% payable
Cancellation request received 8 to 30 working days prior to start date.	50% payable
Cancellation request received within 7 working days of start date.	90% payable

Reschedule timescale	Reschedule fee (% of engagement price)
Re-schedule request received more than 30 working days prior to start date.	0% payable
Re-schedule request received 8 to 30 working days prior to start date.	25% payable
Re-schedule request received within 7 working days of the start date with a firm re-booking date.	50% payable

claranet

Make
modern
happen®