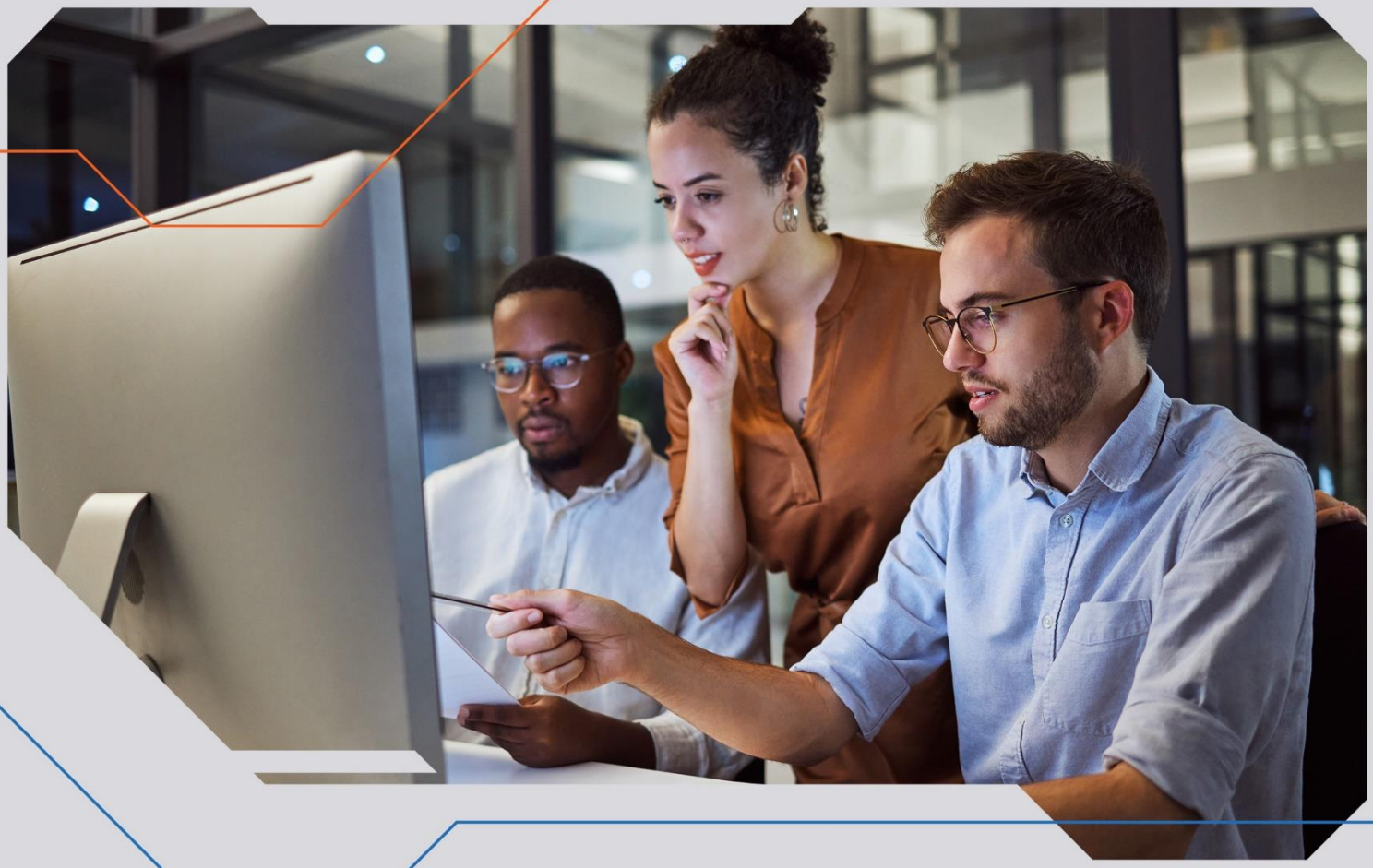

Cyber Essentials

Service Description v2.0 | 12/01/2026

wavenet cyberguard

1. Introduction

Cyber Essentials (CE) and Cyber Essentials Plus (CE+) form a cornerstone of Wavenet CyberGuard's Assurance services, designed to help organisations demonstrate a strong baseline of cyber hygiene in line with the UK government's National Cyber Security Strategy. These certifications are important for any organisation seeking to reduce cyber risk, meet public sector contract requirements, and build trust with customers and stakeholders.

As an IASME-accredited certification body, we offer end-to-end guidance and assessment services for CE and CE+, supporting organisations at every stage - whether they are confident self-certifiers or require hands-on support. Our services are suitable for all organisation sizes and sectors, with tailored delivery based on capability and complexity.

1.1. What does the CE scheme address?

The CE scheme is designed to help organisations protect against a wide range of the most common cyber threats. It focuses on implementing five fundamental security controls that, when properly configured, significantly reduce the risk of an attack:

- Firewalls – to secure internet connections and control incoming and outgoing network traffic.
- Secure configuration – to ensure systems are configured to minimise vulnerabilities and reduce exposure to threats.
- Security update management – to ensure applications and operating systems are updated and protected against known vulnerabilities.
- User access control – to restrict access to data and services based on user roles and responsibilities.
- Malware protection – to defend against malicious software through appropriate antivirus, anti-malware and application controls.

Together, these controls provide a simple yet effective framework for mitigating common cyber-attacks. CE+ builds on this by validating that the controls are not just claimed but operational and effective.

2. CE Service Overview

We provide a comprehensive suite of CE services designed to meet your needs wherever you are on your cyber security journey - from confident, self-sufficient teams to organisations requiring full hands-on guidance and technical audit support.

As an IASME-accredited certification body, we not only deliver certification but add real value through expert-led support, cyber consultancy, remediation advice, and practical insight into achieving and maintaining compliance. Whether you're seeking a cost-effective certification path or needing cyber assurance for regulatory or client requirements, our services scale to fit.

Our CE service portfolio includes three distinct offerings:

- **CE Gap Analysis**: An advisory service that evaluates an organisation's current security posture and controls to identify areas in need of improvement before pursuing a Cyber Essentials certification.
- **Assisted CE Certification**: Our service includes two scheduled half-day sessions of tailored guidance to help you complete the assessment accurately and efficiently. Our assessors act as trusted advisors, helping clarify IASME expectations, avoid delays, and ensuring a smooth path to certification.
- **CE+ Audit and Certification**: A comprehensive audit that validates the implementation of CE controls through technical testing.

2.1. CE Gap Analysis

For many organisations, conducting a CE gap analysis prior to embarking on the CE certification process is a critical step in ensuring organisational readiness and compliance. This exercise provides a comprehensive review of your existing security controls against the CE framework, enabling the identification of deficiencies and vulnerabilities that could lead to certification failure. By addressing these gaps proactively and in advance, your organisation minimises the risk of costly delays or failure during the formal assessment process.

The exercise begins with an assessment of existing technical controls, policies, and configurations, focusing on five key areas: boundary firewalls, secure configuration, access control, malware protection, and patch management. This involves gathering information through document reviews, stakeholder interviews, and technical checks such as vulnerability scans. The aim is to identify where current practices meet, exceed, or fall short of the standard, and to highlight any associated risks.

Once gaps are identified, the analysis provides a detailed report outlining compliance status, weaknesses, and prioritised recommendations for remediation. This often includes an executive summary for leadership and a practical action plan to achieve certification readiness, whether for CE or CE+. Beyond compliance, the process helps reduce exposure to common cyber threats, supports eligibility for certain contracts and insurance, and establishes a roadmap for continuous improvement. In short, a gap analysis is both a diagnostic and strategic exercise, ensuring you are well-prepared to meet recognised security standards and strengthen your overall cyber resilience.

This consultative engagement typically spans two days, subject to the scope of work required. Please note this service is advisory only and does not include IASME certification, for which one of our other CE services is required.

2.2. Assisted CE Certification

Our assisted CE certification service is designed to help organisations confidently complete the CE self-assessment questionnaire and achieve CE certification. This service provides tailored one-to-one guidance from an experienced assessor, delivered through two scheduled half-day remote sessions. The collaborative approach ensures that organisations, especially those new to CE or those who have previously struggled with certification, receive the expert support needed to interpret assessment requirements and clarify IASME expectations.

At the commencement of the engagement, we will register your organisation on the IASME portal and issue you with login credentials. To optimise the value of your dedicated sessions, we will advise you on any data collection or necessary pre-requisites prior to your scheduled appointments.

The assessor will work closely with your team across the two sessions, providing expert advice and practical guidance tailored to your organisation's needs. During each session, the assessor will help you understand the assessment criteria, interpret the requirements, and address any uncertainties regarding the CE framework.

The assessor will offer detailed feedback and actionable recommendations, supporting you in preparing accurate and complete responses to the self-assessment questionnaire. Throughout the process, the assessor will foster a collaborative environment, encouraging open discussion and knowledge sharing to enhance your organisation's cyber hygiene and compliance readiness.

Within 1-3 days of completion of the questionnaire, we will mark your submission and where necessary provide further feedback for a re-submission followed by a second and final marking exercise. If all criteria have been met after either the first or second submission the assessor will award the certificate.

Our service is ideal for organisations seeking a smooth, confident path to CE certification, with the added assurance of expert-led guidance and collaborative support throughout the process.

2.3. CE+ Audit & Certification

CE+ is a higher level of assurance, validating that the five key security controls are operational and effective. Our assessors will determine if you are following the CE guidelines by conducting a comprehensive audit to verify the implementation of the controls through a range of technical testing. During the audit we will perform five mandatory technical tests:

1. External Vulnerability Scan
2. Internal Patch Scan (Credentialed)
3. Malware Protection Validation
4. Multi-Factor Authentication Check
5. Account Separation Review

As a certification body, one of our CE assessors can remotely conduct the audit and award the certificate if you meet all the criteria.

3. Roles & Responsibilities

The following table outlines the expected roles and responsibilities of both parties for each CE service:

Service	Wavenet	Customer
Assisted CE Certification	Register the customer on the IASME portal and issue login credentials. Provide two half-day sessions of 1-to-1 support from an assessor. Offer tailored guidance specific to IASME's expectations and help interpret the questionnaire requirements. Mark the submission within 1–3 working days of submission. Provide detailed feedback and guidance to help the customer complete the process confidently.	Attend the support sessions and engage proactively with the assessor. Complete and submit the questionnaire within 6 months. Ensure all responses are accurate, honest, and reflective of current system configurations. Respond to all assessor feedback and update submissions as needed to meet certification criteria.
CE+ Audit & Certification	Schedule and conduct the CE+ technical audit within 90 days of the CE certification being issued. Perform five mandatory technical tests: 1. External Vulnerability Scan 2. Internal Patch Scan (Credentialed) 3. Malware Protection Validation 4. Multi-Factor Authentication Check 5. Account Separation Review Provide formal findings and prioritised remediation guidance (if required).	Ensure CE+ audit is completed within 90 days of successful CE certification. Provide necessary access to systems, endpoints, infrastructure, and relevant personnel. Implement any remediation work required following the audit within 30 days. Schedule a retest (if required) within the permitted time window.
CE Gap Analysis	Deliver consultancy services with the aim of identifying deficiencies and vulnerabilities. This service is advisory only and does not include IASME certification or assessment services. Engagement time is typically two days subject to the scope of the requirement.	Define the scope of work required from the consultant. Ensure availability of personnel, documentation, or systems necessary to facilitate advisory tasks. Apply the guidance provided as part of the engagement, where appropriate.

4. Assumptions / Pre-Requisites

To ensure a successful engagement, the following assumptions and conditions apply across all Cyber Essentials services:

- You will be expected to read, understand and agree to the IASME Cyber Essentials Terms and Conditions prior to the commencement of any assessment: https://iasme.co.uk/cyber-essentials/terms-and-conditions

- The CE self-assessment questionnaire must be completed and submitted within 6 months of registration on the IASME portal.
- CE+ assessments must be scheduled and completed within 90 days of the successful CE certification date, in accordance with IASME policy.
- In the event of a CE+ failure, you must remediate identified issues and complete a retest within 30 days. Failure to do so will necessitate a full reassessment, at additional cost.
- It is expected that you will be responsible for defining and confirming the scope of systems, users and networks included in the assessment. This scope must be appropriate, accurate, and agreed with us prior to the initiation of any audit or testing activities.
- You will be solely responsible for ensuring the accuracy, completeness and truthfulness of all information and evidence submitted during the assessment process. We will assess submitted materials based on their declared validity.
- Where third-party suppliers, managed service providers, or hosting providers are relevant to the systems in scope, it is expected that you will be responsible for facilitating their cooperation, including timely provision of information and access where required.
- For CE+ technical assessments, all in-scope systems, endpoints, and infrastructure must be available for audit at the agreed times. We will require sufficient access to perform all relevant testing activities.
- Where remediation actions are required (e.g. configuration changes, patching, policy updates), these must be completed by you or your authorised third party. We can provide remediation guidance but are not responsible for implementing changes unless separately contracted.
- In accordance with IASME requirements, our assessors cannot complete or submit questionnaire responses on your behalf. Advisory and assessment services must be delivered separately to maintain independence.
- If you are unsuccessful in your first assessment attempt, the assessor will carry out one further assessment free of any additional charge. Any further assessment attempts will be charged as a new application.
- All our CE services are delivered remotely as standard. Onsite assistance can be provided for an additional charge.

5. Document Information

This service description is a generic, non-contractual document which explains the range of features/benefits and services that may be offered by Wavenet.

The services to be provided will be specified in contractual documentation and where relevant a high-level design. For the avoidance of doubt, Wavenet will have no obligation to provide services set out in this service description.

Versions and releases

Version	Changed by	Date	Details
2.0	Anthony Custy	12/01/2025	First publication