January 2026 – G-Cloud 15

By EG Ltd

Service Definition
Cyber Essentials and Cyber Essentials Plus Advisory Service

1. Service Overview

The Cyber Essentials and Cyber Essentials Plus Advisory Service provide consultancy-led, independent assessment and advisory support to help organisations understand, prepare for, and achieve compliance with the UK Government's Cyber Essentials and Cyber Essentials Plus standards.

The service focuses on security governance, policy, user access, asset management, and effective implementation planning across the Cyber Essentials control areas. The service is advisory only and does not include technical implementation, configuration, or managed security services.

2. Scope of Service

The service includes assessment and advisory support across the Cyber Essentials and Cyber Essentials Plus control areas, including secure configuration, boundary firewalls and gateways, access control, malware protection, and patch management.

Delivery may include documentation and evidence review, system and asset inventory review, stakeholder interviews or workshops, gap analysis against Cyber Essentials requirements, and development of a prioritised remediation and readiness plan. Where required, the service may also include audit readiness support for Cyber Essentials Plus, including guidance on evidence collation and assessment preparation.

3. Service Exclusions

The service does not include technical remediation, system configuration, installation or management of security tools, penetration testing, vulnerability scanning, managed security services, or certification body services.

Responsibility for implementing security controls and submitting certification remains with the customer and their appointed IT providers.

4. Onboarding and Offboarding

Onboarding includes confirmation of scope, certification target (Cyber Essentials or Cyber Essentials Plus), delivery approach, and access to relevant stakeholders, documentation, and system information.

Offboarding includes provision of assessment findings, gap analysis outputs, remediation recommendations, and knowledge transfer as required to support certification submission or audit activities.

5. Service Levels and Support

Support requests related to the consultancy engagement are logged and triaged based on impact and urgency.

Requests are acknowledged within one business day, with time-critical certification-related queries prioritised for same-day response where possible. Service levels relate to consultancy responsiveness only.

6. Service Constraints

Delivery depends on timely access to accurate asset inventories, system documentation, security policies, and relevant stakeholders. Findings represent a point-in-time assessment based on information provided during the engagement.

The service does not guarantee certification, as outcomes depend on the customer's implementation of recommended controls. Services are delivered during agreed business hours, with remote delivery preferred unless otherwise agreed.

7. Security and Confidentiality

All work is conducted in line with industry-standard information governance practices, including confidentiality, secure handling of information, and least-privilege access.

No customer systems are accessed without explicit agreement. No customer data is hosted, processed, or retained beyond the duration of the advisory engagement.

8. Dependencies and Customer Responsibilities

The customer retains responsibility for their systems, data, security controls, and compliance obligations.

Delivery depends on customer engagement, provision of accurate and complete information, and cooperation with internal or third-party IT providers responsible for technical remediation.

9. Exit and Data Access

On completion, all assessment outputs and advisory documentation are provided to the customer. No customer data is retained following service completion.