CAMBRIDGE
CYBER ADVISERS

Security Assurance

Service Definition Document. Version 1.0

19 January 2026

Security Assurance Service Definition Document

1. Introduction

This Service Definition Document describes the Security Assurance service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides ongoing, structured assurance across an organisation's security controls, governance processes, and operational practices to ensure they remain effective, compliant, and aligned to recognised industry standards.

Modern organisations operate in dynamic environments where technology, threats, and regulatory expectations evolve rapidly. Security Assurance ensures that implemented controls continue to function as intended, that risks are proactively identified, and that governance structures remain robust and fit for purpose.

Using a combination of control validation, evidence review, stakeholder engagement, and alignment to frameworks such as NCSC CAF, ISO 27001, and NIST CSF, the service delivers continuous confidence in the organisation's security posture and its ability to withstand emerging threats.

2. Service Overview

The Security Assurance service provides a structured, repeatable approach to validating the effectiveness of security controls, policies, and operational processes. It ensures that security measures are not only implemented but are functioning correctly, consistently, and in line with organisational risk appetite.

The service supports organisations in maintaining compliance, strengthening governance, and ensuring that security capabilities evolve alongside business and technology changes.

Activities include:

- Review of governance structures, policies, and assurance mechanisms
- Assessment of control design and operational effectiveness
- Validation of technical and procedural security controls
- Review of monitoring, detection, and response processes
- Assessment of compliance against internal and external standards
- Identification of risks, gaps, and areas requiring uplift
- Mapping assurance findings to recognised frameworks (e.g., NCSC CAF, ISO 27001, NIST CSF)
- Regular reporting cycles and assurance dashboards
- Executive and operational-level debrief sessions

Service Features

- Comprehensive assurance across governance, people, process, and technology
- Alignment to NCSC CAF, ISO 27001, NIST CSF, and industry best practices
- Control design and effectiveness testing
- Review of identity, cloud, network, and endpoint security controls
- Assessment of SOC, SIEM, EDR, and monitoring capabilities
- Assurance of incident response processes and readiness
- Continuous or periodic assurance cycles
- Assurance dashboards and maturity scoring
- Executive reporting with risk-based prioritisation
- Optional advisory and remediation support

Service Benefits

- Provides continuous confidence in the effectiveness of security controls
- Ensures alignment with regulatory and compliance requirements
- Identifies weaknesses before they impact operations
- Supports governance, risk, and compliance (GRC) functions
- Improves operational resilience and readiness
- Enables informed decision-making based on validated risk insights
- Strengthens organisational security culture and accountability
- Supports long-term strategic security planning

3. Service Scope

The service includes, but is not limited to, assurance of governance structures, control design and effectiveness, operational processes, and compliance alignment. Activities may include policy assurance, identity and access management validation, cloud configuration assurance, network and endpoint control testing, monitoring and detection assurance, and incident response capability review.

4. Delivery Methodology

All CCA engagements follow a phased approach using our standard methodology:

- Scoping and Planning
- Documentation Review and Stakeholder Interviews
- Control and Process Assurance Assessment
- Analysis and Reporting
- Executive and Technical Debrief

5. Deliverables

- Executive Summary Report
- Assurance Findings Report
- Security Control Effectiveness Assessment
- Risk Register and Impact Analysis
- Assurance Dashboard and Maturity Scoring
- Prioritised Remediation Roadmap
- Optional Advisory and Remediation Support Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- Draft assurance report within 10 working days of assessment completion
- Final report within 15 working days
- Weekly progress updates for longer engagements

7. Governance and Assurance

Activities align with NCSC guidance, ISO 27001 principles, NCSC CAF, and the NIST Cybersecurity Framework. Where required, engagements will be managed by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include assurance findings, maturity scoring, risk register, impact assessment, executive summary, remediation roadmap, and optional evidence pack.

Incident Management

The service evaluates incident response capability but does not manage customer incidents.

Disaster Recovery

Not applicable.

Availability

CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time.

8. Security and Data Protection

- Confidential handling of customer data
- UK-based assurance team
- Secure environments for data processing

- Data retained for 30 days then destroyed
- GDPR, NCSC, and ISO 27001-aligned practices

GDPR & Data Privacy

- Personal data minimisation
- DPIA support available
- Findings anonymised unless requested otherwise

Accreditations

- ISO 27001-aligned practices
- NCSC-aligned methodologies

Staff Security Clearance

SC-cleared staff available upon request; BPSS as a minimum for all CCA consultants.

9. Customer Responsibilities

Customers must provide scoping information, documentation, stakeholder access, and support remediation actions.

Technical Requirements

- Scoping information
- Documentation access
- Contact details for key personnel

Supported Browsers/Devices

Not applicable.

Access Restrictions

Customer must designate authorised individuals for scope approval, change requests, access to customer systems and/or services, and receipt of outputs.

10. Service Constraints

Activities are limited to agreed scope and timeframes; some may require controlled windows.

11. Pricing

Pricing is engagement-based and determined by scope, duration, and complexity. Pricing is based on:

- Number and complexity of controls in scope
- Assurance depth (design review, effectiveness testing, or both)
- Environment complexity
- Engagement duration

Typical engagements range from 2–12 weeks depending on assurance breadth.

Day-rate pricing is available on the pricing document and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering is typically completed via Purchase Order following confirmation of service purchase. CCA will invoice at the end of every calendar month, providing a detailed breakdown of services delivered, including VAT/expenses. Consolidated invoices can be provided. Invoices may be issued electronically or via post.

12. Exit and Offboarding

- Assurance findings delivered
- Knowledge transfer completed
- Data destroyed within 30 days (certificate available)

Onboarding

- Requirements workshop
- Scope definition
- Stakeholder identification
- Communication validation

Offboarding

- Walkthrough of assurance findings
- Delivery of reports
- Optional remediation workshop
- Secure data destruction

Training Provided

- Assurance awareness session
- Incident response and governance briefing
- Optional tabletop exercises

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; work completed to date will be invoiced
- Provider may terminate only under defined exceptions (e.g., breach of Rules of Engagement or safety concerns)

14. Contact and Support

A delivery manager is assigned for each engagement. Support is available via email and phone during delivery hours.

Included as standard:

- Email and phone support during the engagement
- Delivery manager assigned
- Access to reporting team for clarifications

Enhanced support packages available for continuous assurance programmes.