CAMBRIDGE CYBER ADVISERS

Security Audit & Assessment

Service Definition Document. Version 1.0

19 January 2026

Security Audit & Assessment

1. Introduction

This Service Definition Document describes the Security Audit & Assessment service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides a structured, comprehensive evaluation of an organisation's security posture across people, processes, and technology, aligned to recognised industry standards and best practices.

Modern organisations face an evolving threat landscape where attackers exploit weaknesses across governance, configuration, identity, cloud, and operational processes. This service provides an independent, evidence-based assessment of an organisation's security maturity, identifying strengths, weaknesses, and priority areas for improvement.

Using a combination of documentation review, stakeholder interviews, technical analysis, and alignment to frameworks such as the NIST Cybersecurity Framework, the assessment delivers a clear, actionable understanding of current security capability and the steps required to enhance resilience.

2. Service Overview

The Security Audit & Assessment service provides a holistic review of an organisation's security controls, governance structures, and operational readiness. The assessment evaluates the effectiveness of existing measures in preventing, detecting, and responding to cyber threats.

This service delivers a structured, end-to-end assessment of security maturity across cloud and on-premise environments. It identifies gaps, risks, and improvement opportunities across all major security domains, including governance, identity, network security, endpoint protection, monitoring, incident response, and data protection.

Activities include:

- Review of policies, processes, and governance structures
- Stakeholder interviews across business and technical teams
- Assessment of technical controls and security tooling
- Evaluation of monitoring, alerting, and incident response capability
- Identification of risks and maturity gaps
- Mapping findings to recognised frameworks (e.g., NIST CSF)
- Detailed reporting with prioritised remediation guidance
- Executive-level and technical debrief sessions

Service Features

- Comprehensive assessment across governance, people, process, and technology
- Alignment to NIST Cybersecurity Framework and industry standards
- Review of identity, cloud, network, and endpoint security controls

- Evaluation of SOC, SIEM, EDR, and monitoring capabilities
- Assessment of incident response readiness
- Maturity scoring across all security domains
- Detailed reporting with actionable recommendations
- Executive summary with risk-based prioritisation
- Optional follow-on advisory and remediation support

Service Benefits

- Provides a clear, evidence-based view of current security posture
- Identifies gaps and weaknesses before they are exploited
- Supports compliance with NCSC guidance, Cyber Essentials Plus, and ISO 27001
- Enhances organisational readiness and resilience
- Improves alignment between security and business objectives
- Enables informed investment decisions based on risk
- Strengthens governance, processes, and operational capability
- Supports continuous improvement and strategic planning

3. Service Scope

The service includes, but is not limited to, governance review, technical control assessment, process evaluation, and maturity scoring. Activities may include policy review, identity and access management assessment, cloud configuration review, network security evaluation, monitoring capability analysis, and incident response readiness assessment.

4. Delivery Methodology

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

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

5. Deliverables

- Executive Summary Report
- Technical Findings Report
- Security Maturity Assessment
- Risk Register and Impact Analysis
- Prioritised Remediation Roadmap
- Optional Advisory and Remediation Support Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- Draft 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, and the NIST Cybersecurity Framework and where required, will be managed by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include findings report, 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 assessment 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 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:

- Scope and number of attack vectors
- Complexity of environments
- Duration of engagement
- Required stealth level

Typical engagements range from 2–8 weeks.

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

Ordering and Invoicing Process

Ordering from clients is generally done via the presentation of a Purchase Order following confirmation of the purchase of a service. CCA will invoice at the end of every calendar month, giving a precise breakdown of the services purchased, including VAT/other expenses. CCA can provide consolidated invoices if required. Invoices can be issued electronically or via post.

12. Exit and Offboarding

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

Onboarding

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

Offboarding

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

Training Provided

- Awareness session
- Incident response 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 testing programmes.