CAMBRIDGE
CYBER ADVISERS

Board Advisory Service

Service Definition Document. Version 1.0

19 January 2026

Board Advisory Service

1. Introduction

This Service Definition Document describes the **Board Advisory** service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. This service provides strategic, high-level cyber risk guidance to executive leadership and boards, enabling informed decision-making, improved governance, and stronger organisational resilience.

Modern organisations operate in an environment of increasing regulatory pressure, evolving cyber threats, and heightened stakeholder expectations. Security is no longer a purely technical concern; it is a core business risk that requires active oversight from senior leadership. CCA's Board Advisory service equips boards with the insight, challenge, and strategic direction needed to navigate this landscape effectively.

Using a combination of expert consultancy, strategic workshops, maturity evaluation, and tailored guidance, the service ensures leadership teams understand their cyber risk exposure, governance responsibilities, and the actions required to strengthen organisational security posture.

2. Service Overview

The Board Advisory service provides expert, business-aligned cyber security guidance to boards, executive committees, and senior leadership teams. It focuses on enabling informed oversight, strategic alignment, and effective governance of cyber risk.

The service delivers structured, ongoing or point-in-time advisory support covering cyber strategy, risk management, governance frameworks, investment prioritisation, and organisational readiness. It ensures leadership teams can challenge assumptions, evaluate risk, and drive meaningful change across the organisation.

Activities include:

- Strategic cyber risk briefings for board and executive members
- Review of governance structures, roles, and responsibilities
- Evaluation of organisational cyber strategy and alignment to business objectives
- Assessment of risk management practices and reporting mechanisms
- Workshops on emerging threats, regulatory expectations, and industry trends
- Guidance on investment prioritisation and programme oversight
- Support in interpreting technical risk information at a business level
- Executive-level and board-level advisory sessions

Service Features

- Expert guidance tailored to the organisation's sector, maturity, and risk profile
- Strategic alignment of cyber security with business objectives
- Independent challenge and assurance for leadership teams
- Support for regulatory and governance expectations
- Insight into emerging threats and industry trends
- Advisory on cyber strategy, investment, and transformation programmes
- Clear, business-focused communication of technical risk
- Optional ongoing advisory retainer for continuous support

Service Benefits

- Strengthens board-level understanding of cyber risk and governance responsibilities
- Enables informed, strategic decision-making
- Improves alignment between security, business priorities, and risk appetite
- Enhances organisational resilience and readiness
- Supports compliance with regulatory and industry expectations
- Provides independent challenge to internal assumptions and reporting
- Helps leadership prioritise investment based on risk and business impact
- Builds long-term strategic capability within the organisation

3. Service Scope

The service includes, but is not limited to, strategic advisory, governance evaluation, leadership engagement, and risk oversight support. Activities may include governance review, cyber strategy assessment, risk reporting evaluation, investment prioritisation guidance, and executive-level workshops.

4. Delivery Methodology

All CCA engagements follow a structured, phased approach:

- Scoping and Planning
- Documentation Review and Leadership Interviews

- Governance and Strategy Assessment
- Analysis and Advisory Reporting
- Executive and Board-Level Debrief Sessions

5. Deliverables

- Board-level Executive Summary
- Strategic Advisory Report
- Governance and Risk Oversight Assessment
- Cyber Strategy Review and Recommendations
- Prioritised Strategic Roadmap
- Optional Ongoing Advisory Retainer Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- Draft advisory outputs within 10 working days of assessment completion
- Final deliverables within 15 working days
- Weekly or monthly progress updates for ongoing advisory engagements

7. Governance and Assurance

Activities align with NCSC guidance, ISO 27001 principles, and recognised governance frameworks. Where required, engagements will be overseen by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include strategic advisory reports, governance assessments, risk oversight analysis, executive summaries, and strategic roadmaps.

Incident Management

The service provides advisory on incident governance but does not manage customer incidents.

Disaster Recovery

Not applicable.

Availability

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

8. Security and Data Protection

- Confidential handling of customer data
- UK-based advisory 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, access to leadership stakeholders, and support for scheduling advisory sessions.

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, and receipt of outputs.

10. Service Constraints

Activities are limited to agreed scope and timeframes; some sessions may require pre-scheduled windows with senior leadership.

11. Pricing

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

- Number of advisory sessions
- Complexity of governance structures
- Duration of engagement
- Requirement for ongoing retainer support

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 is typically via Purchase Order following confirmation of service purchase.
CCA invoices at the end of each calendar month, providing a detailed breakdown of services, including VAT and expenses. Consolidated invoices are available. Invoices may be issued electronically or via post.

12. Exit and Offboarding

- Delivery of all advisory outputs
- 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 strategic planning workshop
- Secure data destruction

Training Provided

- Board-level awareness sessions
- Cyber governance briefings
- Optional tabletop or scenario-based exercises

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; completed work 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
- Dedicated delivery manager
- Access to advisory team for clarifications

Enhanced support packages are available for ongoing advisory retainers.