CAMBRIDGE CYBER ADVISERS

Executive Cyber Tabletop Exercises

Service Definition Document. Version 1.0

19 January 2026

Executive Cyber Tabletop Exercises Service Definition

1. Introduction

This Service Definition Document describes the Executive Cyber Tabletop Exercises service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides a structured, scenario-driven evaluation of an organisation's executive-level cyber crisis readiness, focusing on decision-making, communication, governance, and strategic response capabilities.

Modern organisations face increasingly complex cyber incidents that require coordinated leadership action across technical, operational, legal, and communications functions. This service provides an independent, evidence-based assessment of an organisation's crisis management maturity, identifying strengths, weaknesses, and priority areas for improvement at the executive and senior leadership level.

Using realistic, organisation-specific scenarios, facilitated workshops, stakeholder interviews, and alignment to frameworks such as the NCSC Cyber Incident Response guidance, the service delivers a clear, actionable understanding of executive preparedness and the steps required to enhance organisational resilience.

2. Service Overview

The Executive Cyber Tabletop Exercises service provides a structured, end-to-end evaluation of an organisation's ability to manage and respond to significant cyber incidents at the leadership level. The exercise assesses the effectiveness of governance structures, communication channels, decision-making processes, and cross-functional coordination during a simulated cyber crisis.

This service delivers a tailored, scenario-based exercise designed to test real-world readiness across business, operational, and technical domains. It identifies gaps, risks, and improvement opportunities across incident response governance, executive communication, legal and regulatory obligations, crisis coordination, and strategic decision-making.

Activities include:

- Development of tailored cyber incident scenarios
- Review of existing incident response and crisis management documentation
- Stakeholder interviews across executive, operational, and technical teams
- Facilitation of a structured tabletop exercise
- Evaluation of decision-making, communication, and escalation processes
- Assessment of alignment to NCSC guidance and industry best practice
- Identification of maturity gaps and organisational risks
- Delivery of detailed reporting and improvement recommendations
- Executive-level debrief and optional follow-on workshops

Service Features

- Custom-designed cyber crisis scenarios aligned to organisational context
- Facilitation by experienced cyber crisis and incident response specialists
- Assessment of executive-level decision-making and communication
- Evaluation of crisis governance, escalation paths, and cross-team coordination
- Review of legal, regulatory, and reputational considerations
- Maturity scoring across crisis management domains
- Detailed reporting with actionable recommendations
- Executive summary with risk-based prioritisation
- Optional follow-on advisory, coaching, and remediation support

Service Benefits

- Provides a realistic, evidence-based view of executive cyber readiness
- Identifies weaknesses in crisis governance, communication, and decision-making
- Supports compliance with NCSC guidance and regulatory expectations
- Enhances organisational resilience and crisis preparedness
- Strengthens alignment between leadership, operations, and technical teams
- Enables informed investment and planning decisions
- Improves confidence and capability in managing major cyber incidents
- Supports continuous improvement and strategic risk management

3. Service Scope

The service includes, but is not limited to, scenario development, documentation review, stakeholder engagement, exercise facilitation, and maturity assessment. Activities may include crisis governance review, communication pathway evaluation, decision-making analysis, legal and regulatory considerations, and assessment of incident response integration with executive processes.

4. Delivery Methodology

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

- Scoping and Planning
- Documentation Review and Stakeholder Interviews
- Scenario Development and Exercise Design
- Tabletop Exercise Facilitation
- Analysis and Reporting
- Executive and Technical Debrief

5. Deliverables

- Executive Summary Report
- Detailed Exercise Findings Report
- Crisis Management Maturity Assessment
- Risk Register and Impact Analysis
- Prioritised Improvement 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 exercise 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 recognised crisis management frameworks, 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, improvement roadmap, and optional evidence pack.

Incident Management

The service evaluates crisis 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 follow-on improvement 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:

- Number and complexity of scenarios
- Organisational size and stakeholder groups involved
- Duration of engagement
- Required level of customisation

Typical engagements range from 2–6 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
- Executive crisis response briefing
- Optional follow-on 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.