CAMBRIDGE CYBER ADVISERS

Crisis Management & Cloud Incident Response Readiness

Service Definition Document. Version 1.0

30 January 2026

Crisis Management & Cloud Incident Response Readiness

1. Introduction

This Service Definition Document describes the Crisis Management & Cloud Incident Response Readiness service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. This service helps organisations prepare for, respond to, and recover from cloud-based and hybrid cyber incidents through structured readiness assessments, tabletop exercises, and incident response simulations.

Cyber incidents are inevitable. Our service ensures your organisation is ready to respond effectively, minimising impact and accelerating recovery. We simulate realistic crisis scenarios to test your incident response plans, decision-making processes, and communication strategies under pressure.

2. Service Overview

The Crisis Management & Cloud Incident Response Readiness service delivers structured assessments and simulations to evaluate and enhance an organisation's preparedness for cloud-related cyber incidents. It includes readiness reviews, incident response plan assessments, tabletop exercises, and crisis simulations tailored to your threat landscape and business context.

Activities include:

- Incident response plan review and gap analysis
- Cloud-specific threat scenario development
- Crisis simulation and tabletop exercises
- Stakeholder engagement and decision-making evaluation
- Post-incident analysis and improvement planning

Service Features

- Cloud incident response readiness assessments
- Custom crisis simulation and tabletop exercises
- Stakeholder and executive engagement
- Cloud-native threat scenario development
- Gap analysis of incident response plans
- Post-exercise debrief and improvement roadmap
- Optional Purple Team collaboration for technical validation

Service Benefits

- Improves organisational readiness for cloud-based incidents
- Enhances executive and stakeholder decision-making under pressure

©2026, CCA Ltd

- Identifies gaps in incident response plans and processes
- Strengthens cross-functional collaboration during crises
- Supports compliance with NCSC, ISO 27035, and Cyber Essentials Plus
- Provides actionable insights for resilience improvement

3. Service Scope

The service includes incident response plan reviews, stakeholder interviews, scenario development, simulation delivery, and post-exercise analysis. Scenarios may include ransomware, data breaches, cloud misconfigurations, insider threats, and supply chain attacks.

4. Delivery Methodology

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

- Scoping and Rules of Engagement
- Readiness Assessment and Planning
- Simulation Execution
- Analysis and Reporting
- Executive and Technical Debrief

5. Deliverables

As part of the CCA Cyber Red Teaming & Adversary Simulation service, the following standard deliverables are provided:

- Executive Summary Report
- Readiness Gap Analysis
- Incident Simulation Narrative
- Improvement Roadmap

Additional deliverables can be agreed depending on requirements.

6. Service Levels

The standard CCA delivery SLAs are:

- Engagement commences within 10 working days of contract award
- Draft report within 10 working days of exercise completion
- Final report within 15 working days

©2026, CCA Ltd

- Weekly progress updates for longer engagements

Optional enhanced SLAs available for accelerated delivery Optional enhanced SLAs are available for accelerated engagements or continuous testing.

7. Governance and Assurance

All simulations are conducted under agreed Rules of Engagement. Activities comply with legal, ethical, and safety requirements, and align with CREST and NCSC best practices.

Backup and Restore

Not applicable — this service does not handle customer production data or operate within customer systems in a way that requires backup/restore functionality.

Reporting & Analytics

Outputs include:

- Full attack narrative tracing each stage of compromise
- Detections observed (or missed) during the exercise
- Impact assessment mapped to assets and business functions
- Executive summary with risk scoring
- Full remediation roadmap
- Evidence pack and IoCs (optional)

Incident Management

Controlled escalation paths defined in Rules of Engagement

- Clear escalation paths
- Clear stop/hold procedures
- Real-time escalation to customer security contacts if a genuine issue is detected
- Post-engagement incident response recommendations provided
- Recommendations for incident response

Disaster Recovery

Not applicable — service is not hosted and does not rely on persistent operational infrastructure.

Availability

Service availability applies only to consultant scheduling. CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time with out-of-hours engagements available on request.

©2026, CCA Ltd

8. Security and Data Protection

Customer data is handled confidentially and securely. Data is retained only for the duration necessary to deliver the service and securely destroyed within 30 days of engagement completion. GDPR principles are applied throughout.

- All customer data handled under strict confidentiality
- UK-based testing team available
- Data stored and processed in secure environments
- Data retained for 30 days post-engagement then securely destroyed
- Compliance with GDPR, NCSC guidance, and ISO 27001-aligned practices
- No customer data transferred outside approved jurisdictions

GDPR & Data Privacy

- Personal data used only where strictly required (e.g., targeted phishing scenarios)
- Data minimisation applied
- DPIA support available where necessary
- All findings anonymised unless otherwise requested by customer

Accreditations

- CREST-aligned
- ISO 27001-aligned internal management practices
- Cyber Essentials-aligned

Staff Security Clearance

SC cleared staff available on request. Baseline Personnel Security Standard (BPSS) checks conducted for all consultants.

9. Customer Responsibilities

Customers are responsible for providing accurate scoping information, nominating escalation contacts, supporting internal approvals, and implementing remediation actions.

Technical Requirements

- Defined scoping information (target systems, domains, cloud environments)
- Contact details for incident response and emergency halts
- Customer-supplied threat intelligence (optional)
- Access for briefing key stakeholders (security, IT, SOC)

No agent installation is required unless explicitly scoped.

Supported Browsers/Devices

Not applicable — this is a consultancy service, not a hosted software product.

©2026, CCA Ltd

Access Restrictions

Customer must designate authorised individuals for:

- Scope approval
- Rules of Engagement
- Emergency halt
- Receipt of confidential outputs

10. Service Constraints

Testing activities are limited to agreed scope and timeframes. Physical testing requires prior authorisation. Change freezes or restricted windows may apply.

- All activities require explicitly agreed Rules of Engagement
- Activities must comply with legal, ethical and safety constraints
- Customer must provide accurate escalation contacts and emergency halt procedures
- Physical testing requires property access permissions
- Testing may require change freezes or controlled windows in some environments

11. Pricing

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

- Scope and complexity of attack scenarios
- Complexity of environments
- Duration of engagement
- Number of scenarios
- Required realism and stakeholder involvement

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.

©2026, CCA Ltd

12. Exit and Offboarding

At engagement end, all findings are delivered, knowledge transfer sessions completed, and customer data securely destroyed. Certificates of destruction can be provided.

Onboarding:

- Requirements workshop
- Definition of scope, assets, and Rules of Engagement
- Identification of critical assets, defensive technologies, and response processes
- Validation of communication protocols and escalation points

Offboarding:

- Full walkthrough of all findings
- Delivery of report, evidence and artefacts
- Remediation workshop (optional)
- Secure data destruction within 30 days post-engagement (certificate provided)

Training Provided

- Awareness session
- Incident response readiness briefing
- Optional tabletop exercises with leadership or IT teams
- Resolver team workshops

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.

©2026, CCA Ltd