CAMBRIDGE
CYBER ADVISERS

Security Incident Response

Service Definition Document. Version 1.0

19 January 2026

Incident Response Service Definition Document

1. Introduction

This Service Definition Document describes the Incident Response (IR) service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides rapid, expert-led support to identify, contain, eradicate, and recover from cyber security incidents, while strengthening organisational resilience and ensuring compliance with regulatory and legal obligations.

Modern organisations face increasingly sophisticated cyber threats, including ransomware, data breaches, insider threats, and supply chain compromises. Effective incident response requires a coordinated, evidence-based approach that minimises business impact, preserves forensic integrity, and restores secure operations as quickly as possible.

CCA's Incident Response service combines digital forensics, threat containment, crisis management, and post-incident assurance to deliver a comprehensive, end-to-end capability aligned to NCSC, ISO 27035, and NIST incident handling standards.

2. Service Overview

The Incident Response service provides organisations with immediate access to specialist responders capable of managing the full lifecycle of a cyber incident. The service supports both emergency response and proactive readiness uplift, ensuring organisations are prepared before an incident and supported throughout recovery.

Activities include:

- Initial triage and incident classification
- Threat containment and eradication
- Digital forensics and evidence preservation
- Root cause analysis and attack path reconstruction
- Recovery planning and secure restoration
- Regulatory and legal guidance (e.g., ICO, NCSC reporting)
- Stakeholder and crisis communications support
- Threat intelligence integration and adversary profiling
- Post-incident review and lessons learned
- IR plan development and readiness uplift
- Optional continuous IR support and retainer services

Service Features

- 24/7 incident response activation
- Rapid triage and containment support
- Digital forensics and evidence handling
- Threat intelligence-driven analysis

- Support for ransomware, data breaches, insider threats, and advanced attacks
- Regulatory and legal reporting guidance
- Executive and board-level crisis support
- IR playbook development and readiness uplift
- Post-incident assurance and maturity scoring
- Optional IR retainer for guaranteed response

Service Benefits

- Reduces business impact and downtime during cyber incidents
- Provides expert guidance during high-pressure situations
- Ensures forensic integrity and defensible evidence handling
- Supports compliance with regulatory reporting requirements
- Improves organisational resilience and readiness
- Strengthens governance, processes, and operational capability
- Enables informed decision-making during crisis events
- Supports long-term security improvement and risk reduction

3. Service Scope

The service includes, but is not limited to, incident triage, containment, eradication, recovery support, digital forensics, threat intelligence analysis, crisis management, and post-incident assurance. Activities may include malware analysis, log review, endpoint investigation, cloud incident analysis, network traffic review, and support for regulatory notifications.

4. Delivery Methodology

CCA follows a structured, standards-aligned incident response methodology:

- Activation and Scoping
- Initial Triage and Containment
- Investigation and Forensic Analysis
- Eradication and Recovery Support
- Post-Incident Review and Reporting

5. Deliverables

- Incident Summary Report
- Forensic Findings Report
- Root Cause Analysis
- Threat Intelligence Summary
- Regulatory Reporting Support Pack
- Recovery and Hardening Recommendations

- Post-Incident Review and Lessons Learned
- Optional IR Plan and Playbook Development

6. Service Levels

- Incident activation within agreed SLA (typically 4 hours for retainer customers)
- Draft incident report within 10 working days of investigation completion
- Final report within 15 working days
- Daily or weekly updates during active incidents

7. Governance and Assurance

Activities align with NCSC guidance, ISO 27035 incident management principles, and the NIST Incident Handling Framework. Where required, engagements will be managed by a CCA Project Manager.

Backup and Restore

Not applicable; however, CCA may advise on recovery strategy.

Reporting & Analytics

Outputs include incident reports, forensic findings, threat intelligence summaries, risk assessments, and remediation roadmaps.

Incident Management

CCA manages the cyber security incident response process but does not operate customer ITSM or business continuity processes.

Disaster Recovery

Not applicable; CCA supports recovery planning but does not operate DR services.

Availability

CCA incident responders are available Monday–Friday, 09:00–17:30 UK time, with optional 24/7 retainer coverage.

8. Security and Data Protection

- Confidential handling of sensitive incident data
- UK-based response and forensics team
- Secure environments for evidence processing
- Data retained for 30 days then destroyed
- GDPR, NCSC, and ISO 27001-aligned practices

GDPR & Data Privacy

- Support for breach assessment and notification
- Personal data minimisation
- Findings anonymised unless otherwise required

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 access to systems, logs, stakeholders, and relevant evidence to support investigation and containment.

Technical Requirements

- Access to affected systems and logs
- Contact details for key personnel
- Availability of IT and security teams

Supported Browsers/Devices

Not applicable.

Access Restrictions

Customer must designate authorised individuals for incident activation, evidence access, and approval of containment actions.

10. Service Constraints

Activities are limited to agreed scope and may require controlled windows for containment or recovery actions. Some forensic activities may require system downtime or isolation.

11. Pricing

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

- Incident severity and urgency
- Number of affected systems
- Forensic depth required
- Environment complexity
- Duration of investigation

- Retainer or ad-hoc activation

Typical engagements range from 1–8 weeks depending on incident scale.

Day-rate pricing is available 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

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

Onboarding

- Requirements workshop
- IR readiness assessment (optional)
- Stakeholder identification
- Communication and escalation validation

Offboarding

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

Training Provided

- Incident response awareness session
- Executive crisis management 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 or incident commander 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
- Incident commander assigned
- Access to forensics and reporting teams for clarifications

Enhanced support packages available for 24/7 IR retainers.