Cyber Incident Response Retainer

G-Cloud 15 Service Definition

Table of Contents

Introduction

Ekco Cloud & Security is an ideal partner for public sector organisations seeking a **secure, compliant, and scalable provider** via G Cloud 15.

We make it easier for IT teams to innovate, scale, manage, troubleshoot and secure. Across cloud, business continuity, security and workspace solutions, we enable the growth our customers want with the team they already have.

Through our security-first approach, large specialist workforce, AI-enhanced operations, and proven delivery capability, we help organisations:

- Modernise securely
- Strengthen cyber resilience
- Reduce operational risk
- Improve service continuity
- Deliver safer, more reliable digital services for our customers and their stakeholders.

Ekco's end-to-end cloud and cyber services are well matched to **G Cloud purchasing needs and public sector transformation goals**.

Cyber Incident Response Retainer Service

Service Overview

To support organisations that are seeking to protect their cloud services and prepare themselves against cyber-attacks, Ekco provides an Incident Retainer (IR) Service supported by highly skilled and certified responders to support a customer in preparing and responding effectively to a cyber-incident. The IR Retainer Service can be combined with the Ekco MDR and MXDR service offerings.

Ekco's 24/7 IR Retainer Service utilises leading technology combined with human expertise from the Ekco Cyber Incident Response Team (CIRT) to aid an effective response to a Cyber Incident. Through Ekco's proactive approach to cybersecurity, organisations can minimise the impact of attacks, reduce downtime, and prevent significant financial and reputational damage.

Features

The key features of the Cyber Incident Response Retainer (CIR) Service are:

- 24/7/365 Incident Response Hotline
- Rapid response CIRT SLA
- Retained Bank of Hours for CIR response
- Incident Response Plan Review
- Annual Cyber Simulation Table Top Exercise (TTX)
- Highly certified 'Incident Responders'

Benefits

The key Benefits of the Incident Response Retainer (IR) Service are:

- 24/7/365 Incident Response Hotline with guaranteed SLA
- Provides extended 24/7 on-demand expertise for your organisation
- Provides your organisation with access to highly certified CIRT Team
- Retained pre-paid CIRT Response Hours for use is an emergency
- Ensures organisations are prepared for a Cyber Incident
- Ensures organisations have rehearsed for a Cyber Incident
- Ensures organisations can effectively respond to a Cyber Incident
- Flexible Retainer based offerings with customisable options

Scope

Ekco will carry out the Cyber Incident triage and response activities using reasonable care and skill and in a professional manner utilising the following techniques:

- Preparation / Triage
- Identification & Containment
- Investigation & Analysis
- Eradication & Recovery
- Reporting

The scope of incidents that we are equipped to respond to includes a range of cyber threats such as Ransomware, Malware, Phishing, Business Email Compromise (BEC), Insider Threats, Advanced Persistent Threats (APT), and Unauthorised Access. These categories represent the most common and impactful types of security incidents organisations may face. Our approach covers all critical stages of incident management—preparation, triage, identification, containment, investigation, eradication, recovery, and reporting—ensuring comprehensive support for each type of threat. By addressing these specific incident types, we help organisations effectively detect, manage, and recover from cyber attacks, minimising disruption and safeguarding business operations.

Addon Services Available - Cyber Resilience services.

Basic Readiness

- IR plan review
- Scenario Playbook Development
- Cyber Simulation Exercise (TTX)

Advanced Readiness

- First Responder Training
- Forensic Readiness Review
- Compromise Assessment
- Ransomware Readiness Assessment

Incident Response Advisory

Resilience Assessments

Service Outline

Service Option - Essentials

Ekco Incident Response Retainer Services are designed to be flexible and customisable in order to meet the Customers requirements. The '**Essentials**' Service Level is an IR Retainer Service aimed at small / medium sized organisations to provide reactive and proactive services capability to enable the Customer to both prepare and respond effectively to a Cyber Incident.

- IR Retainer Service Onboarding
- IR Policy & Plan review
- 24/7/365 Incident Response Hotline
- Remote CIRT Response SLA – 4 Hours
- Retained Pre-Paid Credits – 20 Hours
- 5% Discount for retained CIR on rates
- Reuse of Credits for Basic Readiness

Service Option - Standard

Ekco Incident Response Retainer Services are designed to be flexible and customisable in order to meet the Customers requirements. The '**Standard**' Service Level is an IR Retainer Service aimed at medium sized or complex organisations to provide both reactive and proactive services capability to enable the Customer to both prepare, respond and rehearse effectively to a Cyber Incident.

- IR Retainer Service Onboarding
- IR Policy & Plan review
- 24/7/365 Incident Response Hotline
- Remote CIRT Response SLA – 2 Hours
- Onsite CIRT Response SLA – 48 Hours
- Retained Pre-Paid CIRT Response Credits – 40 Hours
- Annual Cyber Simulation Tabletop (TTX) exercise
- 10% Discount for retained CIR on rates
- Re-purpose unused Pre-Paid Hours for use in Cyber Resilience Services
- Annual Rollover of unused Hours – 10%
- Reuse of Credits for Basic & Advanced Readiness

Service Option - Premium

Ekco Incident Response Retainer Services are designed to be flexible and customisable in order to meet the Customers requirements. The **'Premium'** Service Level is an IR Retainer Service aimed at large sized or highly complex organisations to provide a higher level of both reactive and proactive services capability to enable the Customer to both prepare, respond and rehearse effectively to a Cyber Incident.

- IR Retainer Service Onboarding
- IR Policy & Plan review
- 24/7/365 Incident Response Hotline
- Remote CIRT Response SLA – 1 Hours
- Onsite CIRT Response SLA – 24 Hours
- Retained Pre-Paid Credits – 80 Hours
- Annual Cyber Simulation Tabletop (TTX) exercise
- 15% Discount for retained CIR on rates
- Re-purpose unused Pre-Paid Hours for use in Cyber Resilience Services
- Annual Rollover of unused Hours – 20%
- Reuse of Credits for all Cyber Resilience services

Project Implementation

Onboarding a client into their new contracted services requires a structured process to ensure a smooth transition and clear expectations. The following process provides a high-level overview of our bespoke implementation plan.

1. Pre-Implementation Preparation

Initiate internal communications with internal stakeholders, confirming contracted deliverables, and bespoke scope of works. Confirm dedicated resource across the business depending on function.

2. Client Engagement

Initiate communication with the customer's key stakeholders to discuss the onboarding process, timescales (including support go live date), expectations, and roles.

3. Business Intelligence Discovery

Conduct a thorough assessment of the client's internal processes, gather key information regarding end users, business requirements, 3rd party data, user account management and operational workflows.

4. Technical Deliverables

Complete a detailed assessment of the customer's existing IT infrastructure, cloud, network, applications, and systems. Identify different user roles and access requirements. Deploy and document toolsets. Develop a comprehensive knowledge base containing FAQs, troubleshooting guides, and best practices based on their current environment.

5. NOC and SOC Deliverables

Configure and deploy and contracted NOC and SOC toolsets, complete basic security checks such as MFA and password policies.

6. Points of Attention

Based on technical audits and client concerns, create a Points of Attention document with the assigned account manager to review with the client

7. Acceptance into Service

Schedule and complete the acceptance into service with the required internal departments.

8. "Go Live"

Handover to our required internal stakeholders and departments to take on the clients contracted deliverables. Implementation team to provide 2 weeks of enhanced support to our internal teams and the client, ensuring support, access and processes are running smoothly.

Why Ekco

Why UK Public Sector Organisations benefit when they Partner with Ekco Cloud & Security

Security-First Cloud Services Aligned to Government Standards
Ekco Cloud & Security is a leading UK and European **security-first managed cloud provider**, delivering deep expertise across cyber security, identity, and cloud. Our services align with **NCSC guidance, the Cyber Assessment Framework (CAF), NHS DSPT**, and wider public sector assurance requirements.

Our proven **Assess → Protect → Detect → Respond** model supports secure-by-design digital transformation across hybrid and distributed environments—directly addressing public sector risk and resilience priorities.

End-to-End Capabilities Mapped to G Cloud 15
Public sector buyers need suppliers that can deliver migration, protection, management, and optimisation through a single, accountable partner. We provide a **fully integrated cloud and security portfolio**, including:

- Cloud migration and managed cloud operations
- Security and infrastructure management
- Identity security and privileged access management
- Secure modern architecture design
- Real-time threat detection and incident response

These services align directly with **G Cloud 15 lots and purchasing criteria**, enabling organisations to modernise securely while managing complex legacy estates.

Scalable Expertise and Sovereign Delivery
With **1,000+ cloud and security specialists across the UK and Europe**, we offer the scale, depth, and resilience required to support mission-critical public services. A dedicated **identity security practice** provides mature capability for access control and Zero Trust adoption—an increasingly critical requirement across government organisations.

Tailored Solutions for Resource-Constrained Organisations
Recognising the challenges faced by councils, NHS trusts, education, and blue-light services, we offer **cost-effective, scalable cloud and cyber security solutions** designed for organisations with limited internal capacity.

These services protect against phishing, ransomware, and social engineering while meeting G Cloud's expectations for solutions that are secure by default, rapidly deployable, and low overhead.
AI-Enhanced Security Operations
We embed **AI into daily security operations**, improving analyst productivity and response effectiveness. AI-assisted services accelerate:

- Incident triage and prioritisation
- Threat analysis and vulnerability summarisation
- Reporting accuracy and audit readiness

This enables faster outcomes and stronger protection for public bodies operating with limited staffing.

Public Sector-Focused Engagement Model

Our partnership-led approach aligns with government procurement expectations, offering:

- Dedicated, accountable delivery teams
- Transparent SLAs and service reporting
- 24/7 support with local expertise
- Predictable commercial and contract models

This ensures we act as a **strategic long-term partner**, not a transactional supplier.

Global Recognition and Strategic partnerships

These global accreditations partnerships show our commitment to customer satisfaction, data safety, security and overall quality. We're independently audited every year to give our customers confidence in our approach.

From agile managed cloud platforms to next-gen security services that supercharge defences, our local team of specialists provide proactive, round-the-clock management. With one Ekco Cloud & Security team delivering a combination of services, our customers quickly gain control and visibility over their technology.