

Service Definition

Cloud Data and AI Services

G-Cloud 15 - Lot 3: Cloud Support

Supplier: Erisna (trading as London's Own Limited)

Version Date: 28 January 2026

<u>Service Definition</u>	<u>0</u>
<u>Service overview</u>	<u>1</u>
<u>Service categories (Lot 3)</u>	<u>1</u>
<u>What the service includes</u>	<u>2</u>
<u>Core work packages</u>	<u>2</u>
<u>Delivery approach</u>	<u>3</u>
<u>Example delivery lifecycle</u>	<u>3</u>
<u>Technical scope</u>	<u>4</u>
<u>Integration and tooling examples</u>	<u>4</u>
<u>Engagement model, roles and responsibilities</u>	<u>4</u>
<u>Governance</u>	<u>4</u>
<u>Service constraints</u>	<u>5</u>
<u>Support and service management</u>	<u>5</u>
<u>Support channels and availability</u>	<u>5</u>
<u>Support levels</u>	<u>6</u>
<u>Incident management</u>	<u>7</u>
<u>Security and assurance</u>	<u>7</u>
<u>Staff security and clearances</u>	<u>7</u>
<u>Change and vulnerability management</u>	<u>7</u>
<u>Pricing and ordering</u>	<u>8</u>
<u>Service exit and handover</u>	<u>8</u>
<u>Exit activities may include:</u>	<u>8</u>
<u>Contact</u>	<u>8</u>



Service overview

Cloud Data and AI Services is a cloud support service that helps public sector organisations design, deliver, and operate data and AI capabilities. We support programmes end-to-end: discovery, architecture, set-up and migration, integration engineering, governance, and ongoing operational support. Typical outcomes include:

- A clear, delivery-ready roadmap for data and AI improvements.
 - Secure, reliable cloud data foundations (platform set-up, integrations, and migrations).
 - Operational controls for trusted data (quality monitoring, governance processes, and reporting).
 - Improved cost/performance through right-sizing and service optimisation.
-

Service categories (Lot 3)

This service covers the following G-Cloud Lot 3 service categories:

- Cloud Support Services
 - Set Up and Migration
 - Data auditing and organising
 - Data/information structure design
 - Engagement and communication planning
 - Project management and governance
 - Service optimisation/right sizing
 - Mobilisation coordination
 - Other (data and AI operational support as agreed)
-



What the service includes

Buyers can procure the service as discrete work packages, a sprint-based delivery model, or a managed support retainer. Activities, deliverables, and acceptance criteria are agreed upon during mobilisation and captured in a delivery plan.

Core work packages

- Discovery and assessment: current-state review, stakeholder workshops, risk and dependency mapping, and prioritised backlog.
 - Cloud and data architecture: target architecture, security and access patterns, operating model and guardrails.
 - Set-up, integration, and migration: environment provisioning, connectivity, pipeline/build support, and controlled migrations.
 - Data auditing and organising: inventory and classification of data assets, quality profiling, and remediation planning.
 - Data/information structure design: modelling, schema standards, and documentation to support consistent reporting and analytics.
 - Governance delivery: ownership and stewardship model, business rule processes and glossary, and compliance tagging approaches.
 - Operational support: BAU support for in-scope issues, incident triage, performance tuning, and continuous improvement.
-



Delivery approach

Delivery is collaborative and evidence-driven. We work with buyer teams to co-design solutions, implement changes safely, and hand over to BAU (business as usual) with clear documentation.

Example delivery lifecycle

PHASE	WHAT HAPPENS	TYPICAL OUTPUTS
1. Mobilise	Agree scope, stakeholders, environments, access, and plan.	Mobilisation plan; RAID log; communications plan; delivery backlog.
2. Discovery and design	Assess the current state and define the target architecture and controls.	Architecture pack, security approach, migration strategy.
3. Implement	Build, integrate, migrate, and configure agreed components.	Working integrations; migration waves; runbooks; test evidence.
4. Stabilise (hypercare)	Monitor, resolve early issues, and tune performance and reliability.	Stabilisation report; backlog burn-down; updated runbooks.
5. Operate and improve	Ongoing support, optimisation and governance operations.	Service reports; optimisation actions; change backlog.



Technical scope

We support cloud, hybrid, and (where agreed) on-prem environments. Technical tasks are scoped based on the buyer's target platform and delivery approach.

Integration and tooling examples

Where relevant, we can design and implement integrations across common public sector data stacks, including:

- Warehouses and lakehouses: Google Cloud BigQuery, Amazon (AWS) Redshift, Microsoft Fabric, Databricks, Snowflake.
 - Relational and document databases: PostgreSQL, SQL Server, Oracle, MongoDB, Azure Cosmos DB and Azure SQL.
 - ETL/ELT and BI tooling: Apache Airflow, Azure Data Factory, Power BI.
 - Collaboration and alerting: Microsoft Teams, Slack, and email.
 - Identity and security: Microsoft Entra ID, Google SSO.
-

Engagement model, roles and responsibilities

We work in partnership with buyer teams. The buyer typically provides product ownership, access to required environments, and subject matter expertise. Erisna provides delivery leadership, technical specialists, and documentation to support handover and BAU.

Governance

- Weekly delivery checkpoint (progress, risks, dependencies, next steps).
 - Change control is aligned with the buyer's approvals and change windows.
 - Transparent reporting via agreed artefacts (plan, RAID log, decision log).
-



Service constraints

The service is delivered primarily remotely (video calls, email and collaboration tools). On-site delivery is available by agreement and may incur additional costs (e.g., travel and expenses) and must comply with the buyer's site access, security, and working practices. Delivery is dependent on timely access to buyer stakeholders, required technical environments, and any third-party cloud/platform accounts needed to complete agreed activities. Where work involves integration, migration, or changes to live services, delivery is subject to the buyer's change windows, approvals and assurance processes.

Support and service management

Support for Lot 3 covers delivery queries, transition to BAU, and operational assistance for the agreed scope. Support requests are managed via email and an online ticketing process. Phone support is available in business hours. Chat support can be provided through agreed collaboration channels (for example, Microsoft Teams) rather than a web chat widget.

Support channels and availability

CHANNEL	AVAILABILITY / TARGET RESPONSE
Email/ticketing	Response within 24 hours during working hours (09:00 - 17:00, Monday - Friday).
Phone	09:00 - 17:00 (UK time), Monday - Friday.
Web chat	Not provided as a web chat widget (collaboration chat available by agreement).

Our online ticketing support is designed to meet WCAG 2.2 AA accessibility requirements. Users can manage ticket status and priority within the ticketing process.



Support levels

LEVEL	WHAT'S INCLUDED	COST (EX. VAT)
1. Basic	• Email • Support for delivery queries • Mobilisation, coordination and handover during agreed working hours	£0
2. Standard	• Basic support • Ticketing support • Phone • Business-hours coverage • Prioritised response for in-scope BAU issues	£3,000/month
3. Enhanced	• Standard support • Shared support team • Agreed response target • Monthly reporting and recommendations	£5,500/month
4. Dedicated	• Enhanced support • Dedicated Technical Account Manager (TAM) • Fractional Cloud Support Engineer capacity	£14,000/month
5. Mission-Critical	• Dedicated support • Dedicated Cloud Support Engineer • Higher response commitments (scope agreed) • Extended-hours/rota	£32,500/month

Work outside the retained scope (for example, new integrations, migrations, or major changes) is delivered using the published day-rate card or an agreed fixed price.



Incident management

We operate a documented incident management process covering detection, triage, containment, resolution, recovery, and post-incident review. We maintain runbooks for common events (for example, service degradation, failed integrations/jobs, access issues, and suspected security incidents). Users report incidents via email/ticketing, and by phone for high-severity issues. For significant incidents, we provide an incident report that includes a timeline, impact, root cause, and corrective actions.

Security and assurance

Security controls are agreed with the buyer and aligned to the delivery scope. We apply least privilege and role-based access for any administrative access required to deliver the service. Security-relevant activities and actions are logged within the delivery artefacts and (where applicable) buyer systems.

Staff security and clearances

- Staff screening performed to BS7858:2019.
- Government security clearance available up to Security Clearance (SC), where required for the engagement.

Change and vulnerability management

- Changes are assessed for security impact, implemented through controlled change windows, and documented with rollback steps.
 - Vulnerability information is monitored through vendor advisories and security sources, with patches prioritised based on risk and buyer requirements.
-



Pricing and ordering

Buyers can order the service as time-and-materials (day rates) using the published rate card, as a fixed-price statement of work, or as a monthly retainer for ongoing support. The order form will specify roles, rates, deliverables, acceptance criteria, and any agreed-upon expenses for on-site delivery.

Service exit and handover

At the end of the engagement, we provide a structured handover to the buyer. This typically includes documentation, runbooks, architecture artefacts, and a prioritised improvement backlog. Where we have managed operational activities, we support transition to the buyer's BAU team or an alternative supplier by sharing agreed service reports and operational procedures.

Exit activities may include:

- Final service report covering work completed, outcomes achieved, and outstanding actions.
 - Secure return or deletion of any buyer data provided for delivery, in line with contractual requirements.
 - Revocation of Erisna access to buyer environments and rotation of any shared credentials/tokens (as applicable).
-

Contact

Primary support and engagement contacts are agreed in the order form. Support requests are raised via the agreed email address and/or ticketing process.