G-Cloud 15 Service Definition

Lot 3: Cloud Support Services

Service Name: Cloud Data Auditing & Structure Design

1. Service Overview

Cloud Data Auditing & Structure Design is a specialist cloud support service that helps public sector organisations assess, organise and design data for effective use in cloud environments.

The service focuses on understanding existing data assets, identifying quality, structure and governance issues, and designing information structures that support secure cloud adoption, analytics and AI use cases. The service is advisory and delivery-support focused and does not include hosting, operation or management of production systems.

2. Core Functionality & Scope

The service provides specialist support across data assessment, organisation and structure design activities. Typical activities include:

- Auditing data quality, completeness and consistency across datasets.
- Reviewing existing data models, schemas and information structures.
- Analysing data lineage, ownership, dependencies and usage.
- Assessing data governance, metadata and documentation practices.
- Identifying data risks, gaps and constraints affecting cloud use.
- Designing analytics- and AI-ready data structures and models.
- Aligning data structures to cloud platforms and integration patterns.
- Producing clear recommendations, artefacts and design documentation.

The service supports customer delivery teams and cloud platforms but does not include full data migration execution or ongoing operational support.

3. Service Levels

This service is a professional cloud support and advisory offering rather than a managed operational service. Traditional service level agreements (SLAs) for system availability, uptime or incident response do not apply.

Delivery is normally provided during UK business hours (Monday to Friday, 09:00–17:30, excluding public holidays), unless otherwise agreed in the Call-Off Contract. Response times, delivery milestones and review points are agreed as part of the statement of work.

A named delivery lead or technical specialist may be assigned to coordinate activities and provide progress updates throughout the engagement.

MISSION DECISIONS

4. Onboarding & Offboarding Support

Onboarding

Onboarding typically includes:

- Discovery sessions to confirm objectives, scope and success measures.
- Review of relevant documentation, data inventories and architectures.
- Agreement of deliverables, timelines and ways of working.
- Identification of access requirements to data, environments and tools, subject to customer security approvals.

Offboarding

Offboarding support includes appropriate documentation and knowledge transfer, such as data audit findings, structure designs and recommendations.

Any access to customer systems or environments is removed in line with customer instructions at the end of the engagement. Mission Decisions does not retain customer production data beyond what is required for delivery and audit obligations.

All documentation and deliverables can be provided in accessible formats on request, in line with public sector accessibility requirements.

5. Data Management, Backup & Business Continuity

Mission Decisions does not operate or host customer production environments under this service. Responsibility for backup, restore, disaster recovery and business continuity of production systems and data remains with the customer and/or their hosting providers.

Where limited working copies of data are required to support assessment or design activities, this is done in accordance with customer instructions and information governance requirements. Data is stored securely, access-controlled, and retained only for as long as necessary to support the engagement.

Mission Decisions maintains internal business continuity arrangements to support continuation or recovery of professional services in the event of disruption.

6. Service Constraints

- The service is delivered primarily remotely using secure collaboration tools.
- The service does not include hosting, operation or management of production systems.
- Full data migration execution and ongoing operational support are out of scope unless agreed separately.
- Access to data and environments is subject to customer security and approval processes.
- Delivery depends on timely access to relevant data, documentation and stakeholders.

7. Technical Requirements

Technical requirements vary by customer environment but typically include:

- Access to agreed data sources or representative data samples.
- Access to relevant cloud, development or analytics environments where required.
- Access to collaboration tools such as email, video conferencing and shared repositories.

Mission Decisions works within the customer's existing technical standards and policies and does not mandate specific vendors or products.

8. Outage & Maintenance Management

Mission Decisions does not manage outages or maintenance for customer production systems. These are handled by the customer and/or their hosting providers. If outages or maintenance prevent access to data or environments required for delivery, Mission Decisions will work with the customer to reschedule activities and minimise impact on agreed milestones.

Any disruption to Mission Decisions' own delivery or collaboration tooling is managed internally, with customers informed where delivery is materially affected.

9. Hosting Options & Locations

This service does not include hosting of customer production systems or cloud infrastructure. Mission Decisions does not host or operate customer production systems or live service data as part of this service, unless explicitly agreed for limited, short-term delivery or analysis purposes, and documented within the Call-Off Contract.

Where Mission Decisions uses its own tooling for analysis, documentation or collaboration, these services are provided by reputable suppliers with data typically hosted within the UK or EEA, or under appropriate data protection safeguards. Where required, delivery can take place entirely within the customer's own environments and tooling.

10. Security

Mission Decisions applies security-by-design and least-privilege principles throughout service delivery. The organisation holds Cyber Essentials certification and aligns its practices with recognised information security good practice.

Security controls include role-based access, secure authentication, controlled handling of data, and compliance with UK GDPR and the Data Protection Act 2018.

All staff supporting public sector engagements are UK-based. Where required, staff can operate under BPSS, SC or DV clearance, subject to customer requirements and approvals.

11. After-Sales & Ongoing Support

This service does not include a standing service desk, ticketing system or 24/7 operational support. Follow-on advisory or delivery-support engagements can be provided where customers require additional assistance after completion of the initial work.
Any follow-on support is agreed through a new Call-Off Contract or contract extension.

12. Ordering & Invoicing Process

Customers can procure this service via the G-Cloud 15 framework under Lot 3 (Cloud Support Services).

A Call-Off Contract and statement of work define scope, deliverables, timelines and pricing. Pricing is typically based on time and materials using agreed day rates, or fixed-price work packages where requirements are sufficiently defined.

Invoicing is normally monthly in arrears or on completion of agreed milestones, in line with the Call-Off Contract.

13. Termination

Termination is governed by the G-Cloud 15 Framework Agreement and the applicable Call-Off Contract.

On termination or expiry, Mission Decisions will complete agreed handover activities, return or securely delete customer data, and support knowledge transfer as defined in the Call-Off Contract.

14. Roles & Responsibilities

Mission Decisions is responsible for providing suitably skilled personnel, delivering agreed outputs with reasonable skill and care, and complying with applicable legal, security and information governance obligations.

The customer is responsible for operating and managing its own cloud environments and data, granting appropriate access, and ensuring that any actions taken based on recommendations are implemented securely and in line with organisational governance.