Managed Cloud – Service Definition Document

G-Cloud 15: Lot 3 – Cloud Support

1. Service Overview

Our Managed Cloud Services enable public sector organisations to maintain secure, reliable, and cost-effective cloud infrastructure spanning on-premises environments, public cloud platforms (AWS, Azure, GCP), and hybrid architectures. We deliver infrastructure operations including architecture design, security and compliance management, performance monitoring, incident response, and infrastructure automation.

Effective cloud infrastructure management balances day-to-day operational needs with strategic objectives. Our service combines responsive support for incidents with ongoing cost optimisation, capacity planning, security hardening, and performance tuning, ensuring infrastructure meets evolving business requirements while maintaining operational stability.

We work collaboratively with buyers to understand their operational context, compliance obligations, and business priorities. Through assessing existing infrastructure and identifying improvement opportunities, we establish appropriate governance and service level frameworks shaped by organisational risk appetite, budgetary parameters, and strategic direction.

Infrastructure as Code forms a cornerstone of our delivery methodology. Using Terraform, Bicep, ARM templates, and CloudFormation, we ensure infrastructure deployments are consistent, version-controlled, and repeatable. Where appropriate, we implement container orchestration using Kubernetes and Docker. These practices enhance deployment reliability, eliminate manual errors, and allow infrastructure to scale efficiently while preserving security controls.

Our engineers address the full spectrum of cloud infrastructure: compute resources, storage systems, network architecture, security controls, backup solutions, and disaster recovery capabilities. Service delivery occurs within buyer-controlled environments, integrating with established operational workflows.

The following services are included:

- **Managed Private Cloud**
  - **Managed Private IaaS -** Operations and support for on-premises infrastructure including networking, virtualization, compute, storage, operating systems, and patch management
  - **Managed Private SaaS/PaaS -** Database management, middleware operations, and platform services in dedicated environments
  - **Application management -** Deployment, monitoring, performance tuning, and maintenance of applications on private infrastructure
- **Managed Public Cloud**
  - **Managed Public IaaS -** Infrastructure operations and optimization across AWS, Azure, and GCP including compute instances, storage, networking, and security configuration
  - **Managed Public SaaS/PaaS -** Container orchestration with Docker and Kubernetes, managed database services, and serverless platform management
  - **Application management -** Cloud-native application deployment, scaling, monitoring, and lifecycle management
- **Managed Hybrid Cloud**
  - **Managed Hybrid IaaS** - Architecture design and operations spanning on-premises and public cloud environments with consistent infrastructure management

- **Managed Hybrid SaaS/PaaS -** Platform services and workload orchestration across hybrid environments
- **Application management** - Application deployment and operations across distributed hybrid infrastructure

This service offering is suitable for public sector organisations that:

- Operate cloud, on-premises, or hybrid infrastructure requiring ongoing management
- Need reliable operational support to maintain service availability and performance
- Require assurance over infrastructure security, resilience, and compliance
- Want to reduce operational risk through proactive monitoring, optimisation, and incident management

2. Service Delivery

Service delivery begins with an operational assessment of the buyer's existing cloud, on-premises, or hybrid environments. This establishes a clear understanding of current infrastructure, platform services, operational processes, service dependencies, and risk areas. The assessment informs priorities for stabilisation, optimisation, and ongoing management, ensuring support activities are aligned with service criticality and organisational objectives.

We define and agree appropriate operational models covering monitoring, incident management, change control, access management, and routine maintenance. These models are tailored to the buyer's governance structures, risk appetite, and compliance obligations, providing clarity of roles, responsibilities, and escalation paths.

Engagement and communication planning is embedded throughout service delivery to ensure stakeholders remain informed of service performance, planned activities, incidents, and improvement initiatives. Regular reporting and service reviews support transparency and enable informed operational and strategic decision-making.

Operational governance and service management processes are applied to coordinate day-to-day support activities, manage risks, track service performance, and maintain alignment with agreed service levels. Clear reporting mechanisms, service metrics, and review cycles are established to support accountability and continual improvement.

Proactive optimisation activities are performed to ensure infrastructure and platform services remain efficient, resilient, and cost-effective. This includes capacity planning, performance tuning, configuration reviews, and cost management activities, balancing operational stability with evolving demand.

Service mobilisation ensures that monitoring tools, access controls, support processes, and integration with existing operational workflows are established before full service commencement. This enables a smooth transition into managed operations with minimal disruption to live services.

Buyers benefit from a structured and reliable approach to cloud operations, with improved service availability, reduced operational risk, and greater visibility of infrastructure performance and costs. Clear governance and proactive management support service continuity while enabling controlled change and optimisation over time.

Services can be delivered remotely or on-site by experienced cloud infrastructure engineers, according to buyer requirements, preferences, and location. Delivery arrangements are agreed prior to Call-Off Contract signing.

3. Service Constraints

Delivery is dependent on timely access to relevant systems, documentation, and stakeholders. Scope is limited to the services agreed in the Call-Off Contract.

4. Roles Involved

Services are delivered by experienced Infrastructure Engineers and Infrastructure Operations Engineers. A Delivery Manager can be provided as a single point of contact where required.

5. Onboarding and Offboarding

Onboarding includes access setup, scope confirmation, and security briefing. The kick-off meeting will take place within 5 working days of Call-Off signature.

Offboarding includes knowledge transfer and handover of deliverables.

6. Certifications

- ISO 9001:2015 Quality Management System
- ISO 14001:2015 Environmental Management System
- ISO/IEC 20000-1:2018 IT Service Management system
- ISO/IEC 27001:2022 Information Security Management System
- Cyber Essentials Certificate of Assurance