Waracle Ltd. - G-Cloud 15 Lot 3 Service Definition

Service: Managed DevOps, Cloud Operations, and FinOps Support

This document serves as the formal Service Definition for the Waracle Ltd. **Managed DevOps, Cloud Operations, and FinOps Support** service, listed under G-Cloud 15 Lot 3: Cloud Support Services.

---

1. Service Overview and Scope

Element	Description
Service Name	Waracle Managed DevOps, Cloud Operations, and FinOps Support
Lot 3 Category	**Ongoing Support** (Primary), **Quality Assurance and Performance Testing**, and **Security Services**
Service Description	A fully managed 24/7 service providing operational support, maintenance, and continuous optimisation for client-owned cloud platforms (AWS, Azure, GCP). This service guarantees platform stability, security, and cost efficiency using DevSecOps and Site Reliability Engineering (SRE) principles. Delivered by UK-based, certified engineers.
Target Audience	Public sector organisations (including Central Government, NHS, Local Authorities) requiring skilled, continuous support for their mission-critical, production cloud environments after the initial build/migration phase.
Key Supported Technologies	AWS, Microsoft Azure, Google Cloud Platform (GCP). Support covers IaaS, PaaS, Kubernetes/Container Orchestration, monitoring/logging tools (e.g., Splunk, Prometheus), and IaC tooling (e.g., Terraform).
Location of Service Delivery	UK-based, remote delivery model with on-site deployment or critical incident support available when agreed upon in the Statement of Work (SOW).

Service Scope: Inclusions and Exclusions

Area	Inclusions (What Waracle Will Do)	Exclusions (What This Service Does NOT Cover)

Operations (Run)	24/7/365 proactive monitoring; Incident response, triage, and resolution; Management of platform capacity, scaling, and backups; Routine patch management.	Bespoke application code development, bug fixing, or feature enhancement (refer to DOS framework); Major system re-architecture projects; Third-party software licensing management.
Security & Compliance	Management of platform security configuration; Vulnerability scanning and remediation of known CVEs; Compliance monitoring for established security controls; Access and Identity Management (IAM) governance.	Forensic security investigation; Full penetration testing (separate service); End-user application support (L1 support).
Optimisation	Continuous FinOps (Cost Optimisation) activities; Performance monitoring and tuning; Management of infrastructure-as-code (IaC) repository and drift detection.	Ownership of the customer's internal change/governance process; Commercial negotiation with cloud hyperscalers.

---

2. Service Level Agreements (SLAs) and Key Performance Indicators (KPIs)

Waracle provides the following service levels to ensure the reliability and performance of the managed service.

Metric	Definition	Service Level Guarantee
P1 Critical Incident	Unplanned complete service outage or major security breach.	Response Time:**15 minutes** Resolution Target: **4 hours**
P2 High Incident	Partial service degradation or severe security warning.	Response Time: **30 minutes** Resolution Target: **8 hours]**
P3 Standard Request	Routine requests or minor non-service impacting issues.	Response Time: **4 hours**

		Resolution Target: **3 business days**
Platform Availability	Guaranteed uptime of the core managed platform infrastructure.	**99.9%** (Excluding planned maintenance windows)
Patching Timeframe	Time to apply critical security patches (CVEs) upon release.	**Within 7 days of vendor release**
FinOps Target	Commitment to identify savings opportunities per quarter.	Target: **Identify 10%** of managed spend savings.

3. Outcomes and Deliverables

ID	Deliverable Title	Description and Format
D11	**Monthly Service Report**	Comprehensive report detailing platform performance against agreed SLAs and KPIs, incident summaries, security patch status, and capacity usage. Delivered as **PDF Report and Review Meeting**.
D12	**Cloud Cost Optimisation (FinOps) Report**	Monthly analysis of cloud expenditure, identifying areas of waste, under-utilised resources, and recommending specific actions to reduce running costs.
D13	**Managed Infrastructure-as-Code (IaC) Repository**	Continuous management and maintenance of the IaC code base (e.g., Terraform), ensuring code remains up-to-date, secure, and documented.
D14	**Cloud Security Posture Management (CSPM) Audit Summary**	Quarterly summary of the platform's security compliance, detailing any configuration drift from the established secure baseline and remediation actions taken.
D15	**Runbook and Operations Manual Updates**	Maintenance and continuous update of the operational documentation required for platform management, ensuring accuracy for client handovers.

4. Pricing and Commercial Model

This service allows for a predictable operational expenditure model.

Element	Description
Pricing Model	**Retainer/Managed Cost Model** based on the size and complexity of the managed platform (e.g., fixed fee per service component or percentage of managed cloud spend). Additional **Time & Materials (T&M)** rates apply for non-scheduled engineering requests (project work, major upgrades).
Rate Card Reference	All current G-Cloud 15 compliant day rates for specialist roles (DevOps Engineer, SRE, etc.) are detailed in the accompanying official document: **Waracle Ltd G-Cloud 15 Pricing Document**.
Invoicing	Invoiced **monthly in arrears** via electronic invoice.
Expenses	All standard remote operational costs are included in the monthly fee. **Agreed on-site visits / travel expenses will be billed at cost and in line with HMT guidance**.
Minimum Term	The minimum initial term for this managed service is **3 months** to allow for effective onboarding and toolset integration.

---

5. Service Management and Transfer

Element	Description
Support Hours	**24/7/365** coverage is provided for P1/P2 critical incidents. Standard operational/change work hours are **Monday to Friday, 9:00 AM - 5:30 PM GMT/BST.**
Service Desk	Access to a dedicated UK-based service desk via phone, email, and integrated ticketing system **e.g., ServiceNow, Jira Service Desk]**.
Client Responsibilities	Buyer must maintain current cloud subscription, provide administrative access to the relevant cloud tenants, and promptly communicate critical business context or policy changes.

Onboarding	A formal transition-in period of **2 weeks** is required to install monitoring agents, baseline the environment, and integrate with client processes.
Exit / Offboarding	A formal offboarding period of **90 calendar days** is required. Waracle will transition all access credentials, runbooks (D15), IaC code (D13), and monitoring configurations to the buyer or a nominated successor supplier.

---

6. Technical and Security Standards

Element	Description
Security Standards	Waracle holds current **Cyber Essentials Plus / ISO 27001 Certification**. All managed environments are maintained in compliance with the NCSC Cloud Security Principles.
Security Clearance	Waracle can provide personnel holding **BPSS / SC Clearance** for relevant engagements, subject to client requirements and resource availability.
Backup & Resilience	Management of backup schedules and disaster recovery replication is performed in accordance with the client's RPO (Recovery Point Objective) and RTO (Recovery Time Objective) requirements.
Data Handling	All data processed during the engagement will be handled strictly in accordance with UK GDPR, the Data Protection Act 2018, and the terms of the G-Cloud framework agreement.