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

Service: Cloud Platform Quality Assurance and Performance Testing

1. Service Overview and Scope

Element	Description
Service Name	Waracle Cloud Platform Quality Assurance and Performance Testing
Lot 3 Category	**Quality Assurance and Performance Testing** (Primary), **Security Services**, and **Ongoing Support**
Service Description	An independent assurance service verifying the resilience, performance, and operational stability of client cloud platforms (AWS, Azure, GCP). Services include testing load capacity, identifying performance bottlenecks, validating security controls, and assuring compliance against service level agreements (SLAs) and design specifications.
Target Audience	Public sector teams requiring independent verification of mission-critical services, including technical teams prior to Go-Live, and operational teams seeking ongoing resilience testing.
Delivery Methods	Project-based, outcome-driven engagement using specialist testing toolsets and automated scripting (e.g., dedicated load testing, chaos engineering).
Location of Service Delivery	UK-wide remote delivery, with a collaborative approach to test environment setup and data access.

Service Scope: Inclusions and Exclusions

Area	Inclusions (What Waracle Will Do)	Exclusions (What This Service Does NOT Cover)
Performance Testing	Full testing cycle including Test Strategy Definition, Load Profile Generation, Execution of	Full Application Development (only testing the deployed cloud platform); Long-term performance monitoring (covered under Managed DevOps

	Load/Stress Tests, and detailed Bottleneck Identification.	service); Licensing fees for non-standard testing tools.
Quality Assurance (QA)	Validation of infrastructure-as-code (IaC) against standards; Testing of disaster recovery (DR) procedures and failover mechanisms; Verification of configuration and security controls.	Remediation of code defects or architectural flaws (recommendations provided, but fix execution is separate); End-user acceptance testing (UAT) planning.
Security Assurance	Security Configuration Auditing; Testing of Identity and Access Management (IAM) controls; Verification of patching and vulnerability management processes.	Full Penetration Testing (separate specialist service); Live security incident response (covered under Managed DevOps service).

---

2. Testing Methodologies and Outcomes

Activity Type	Description	Key Outcome/Deliverable
Performance Testing	Simulating high-volume user traffic (load/stress) to determine the platform's breaking point, latency, and throughput capabilities under pressure.	**Performance Testing Report:** Detailing test execution, identified bottlenecks, and recommendations for performance tuning.
Resilience Testing	Executing controlled failures (e.g., node shutdown, network disruption) to validate the platform's High Availability (HA) features and the Recovery Time Objective (RTO) against the SLA.	**Resilience Validation Report:** Confirmation that RTO/RPO targets are met, and detailing any configuration flaws impacting recovery.
Configuration Audit	Automated and manual review of cloud resource configurations against the client's Security Policy, governance standards, and industry best practices (e.g., NCSC).	**Configuration Audit Report:** Scorecard of compliance against baseline, with detailed findings and prioritised recommendations for remediation.

SLA Verification	Testing key operational metrics (e.g., logging effectiveness, monitoring coverage) to verify the ability of the Buyer and Waracle's ongoing support teams to meet agreed SLAs.	**Service Reliability Report:** Confirmation of operational readiness and measurement against defined KPIs.

3. Outcomes and Deliverables

ID	Deliverable Title	Description and Format
D20	**Test Strategy and Plan Document**	Comprehensive plan outlining scope, acceptance criteria, test environments, data requirements, and load profiles, delivered pre-execution.
D21	**Test Execution and Results Report**	Consolidated technical report detailing all performance, resilience, and security audit findings, including clear severity classifications and technical impact analysis. Delivered as **PDF Report and Formal Presentation**.
D22	**Remediation Recommendations Log**	Prioritised, actionable log of all identified flaws and necessary configuration changes required to secure or stabilise the platform.
D23	**Automated Testing Assets**	Handover of all non-proprietary testing scripts, load profiles, and automated test frameworks used during the engagement for client re-use.

4. Pricing and Commercial Model (Reference)

Element	Description
Pricing Model	Primarily **Time and Materials (T&M)** based on specialist roles (Test Architect, Performance Engineer) and duration, OR **Fixed Price** for clearly defined and bounded audit projects (e.g., a 4-week Pre-Go-Live Assurance Audit).

Rate Card Reference	All current G-Cloud 15 compliant day rates for specialist roles are detailed in the accompanying official document: **Waracle Ltd G-Cloud 15 Pricing Document**.
Invoicing	Invoiced **monthly in arrears** for T&M or upon the achievement of agreed-upon milestones for Fixed Price engagements.
Tooling Costs	Where Waracle uses proprietary testing toolsets, costs are **included in the day rate / Billed separately at cost dependent upon the tools deployed, pre-agreed with the client.** .

5. Service Management and Transfer

Element	Description
Service Availability	Testing services are delivered during standard UK business hours (M-F, 9:00 AM to 5:00 PM), unless out-of-hours load testing windows are specifically agreed upon in the SOW to minimise impact on live services.
Project Management	Delivery adheres to an agile methodology, with joint planning sessions with the Buyer's technical team to ensure minimal disruption to the development or operations pipeline.
Security Clearance	Waracle personnel will hold the necessary security clearances, as detailed in the SOW **e.g., BPSS, SC**.
Knowledge Transfer	Formal review and handover of all testing scripts (D23) and methodology to the Buyer's internal QA or DevOps team upon completion.

6. Technical and Security Standards

Element	Description
Accreditation	Waracle holds **Cyber Essentials Plus / ISO 27001 Certification**.

Testing Standards	All testing protocols adhere to industry standards (e.g., NIST, ISTQB) and conform to the NCSC Cloud Security Principles and OWASP standards where applicable.
Data Handling	All testing is conducted using non-live, sanitised, or production-like data, as explicitly agreed upon with the Buyer. Waracle guarantees strict adherence to UK GDPR and data protection policy when accessing any data.
Deliverable Accessibility	All final reports (D21) and documentation are provided in **WCAG 2.1 AA compliant formats**.