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

Service: Cloud Security and Governance Assurance

1. Service Overview and Scope

Element	Description
Service Name	Waracle Cloud Security, GRC, and Compliance Assurance
Lot 3 Category	**Security Services** (Primary), **Planning**, and **Quality Assurance and Performance Testing**
Service Description	An independent assurance service providing comprehensive Governance, Risk, and Compliance (GRC) consulting. We assess, audit, and remediate cloud security postures (AWS, Azure, GCP) to ensure strict adherence to public sector security mandates, including NCSC guidance, ISO 27001, and the Public Sector Contract (PSC) requirements.
Target Audience	Public sector Chief Information Security Officers (CISOs), Risk/ Compliance teams, and cloud platform owners requiring external validation of security controls and clear remediation roadmaps.
Key Supported Technologies	AWS, Azure, GCP, Kubernetes, Identity Management Systems (e.g., Azure AD, IAM), Cloud Security Posture Management (CSPM) tools.
Location of Service Delivery	UK-based, flexible delivery model utilizing remote access and agreed-upon secure channels for data and document sharing.

Service Scope: Inclusions and Exclusions

Area	Inclusions (What Waracle Will Do)	Exclusions (What This Service Does NOT Cover)
Assessment & Audit	Cloud Security Architecture Review; GRC Maturity Assessment; Policy and Control Mapping against standards (ISO/NCSC); **e.g., Azure Well-Architected Review.**	External, licensed Penetration Testing (Waracle provides internal vulnerability scanning and remediation advice); Management of client-owned security licenses; Execution of non-security related cloud fixes.

Governance & Policy	Definition of a Cloud Security Operating Model; Drafting/Review of security policies and procedures; Advice on Identity and Access Management (IAM) controls; Data classification and protection strategy.	Legal representation for data breaches; Ongoing enforcement of compliance post-engagement (covered by Managed Support service); Staff training (covered by Training service).
Remediation & Assurance	Prioritised remediation backlog and actionable advice; Configuration checks against best practice baselines; Compliance reporting for internal and external audits.	Responsibility for the client's failure to implement agreed remediation actions; Purchase of security hardware or physical security services.

2. Audit and Assurance Methodologies

Waracle uses a structured methodology, tailored to the security classification of the Buyer's data (e.g., OFFICIAL), to deliver measurable security outcomes.

Methodology	Description	Focus of Assessment
Baseline Audit	Reviewing the platform against mandatory minimums, such as **Cyber Essentials Plus** and the client's internal security policy.	**Compliance** and **Hygiene**
Control Mapping	Mapping existing cloud controls (technical, administrative) against required frameworks (e.g., ISO 27001, NCSC Cloud Security Principles).	**Risk Coverage** and **Policy Adherence**
Remediation Planning	Delivering a clear, prioritised backlog of security and governance findings, classifying risks by severity (High, Medium, Low).	**Actionability** and **Impact**
Operating Model Review	Assessing the organisational structure, roles, and responsibilities for security management (e.g., security incident process, change management).	**Operational Readiness** and **Efficiency**

3. Outcomes and Deliverables

The service produces formal, defensible documentation essential for regulatory compliance.

ID	Deliverable Title	Description and Format

D29	**Cloud Security and GRC Audit Report**	The primary deliverable: a comprehensive report detailing current security posture, identified vulnerabilities, and non-compliance findings, scored against severity. Delivered as **PDF Report and Executive Summary Presentation**.
D30	**Remediation Prioritisation Roadmap**	A prioritised, actionable backlog of security fixes, configuration changes, and policy implementations required to close identified gaps, including estimated effort and necessary skill sets.
D31	**Target Security Operating Model (SecOps)**	Documentation defining the future state of security governance, detailing roles, responsibilities, process flows, and key controls for maintaining compliance.
D32	**Security Policy/ Standards Gap Analysis**	Formal document identifying where existing client policies fail to meet industry standards (ISO 27001 / NCSC) or the requirements of the specific cloud platform.

4. Pricing and Commercial Model (Reference)

This is a professional consultancy service, typically billed based on the specialized personnel required for the audit and planning period.

Element	Description
Pricing Model	Primarily **Fixed Price** for defined audit outcomes (e.g., a 6-week GRC Assessment). Time & Materials (T&M) based on day rates applies for policy drafting or specific remediation planning.
Rate Card Reference	All current G-Cloud 15 compliant day rates for specialized roles (Security Architect, GRC Consultant, Lead Auditor) are detailed in the accompanying official document: **Waracle Ltd G-Cloud 15 Pricing Document**.
Invoicing	Invoiced **50% upon SOW signature, 50% upon final Deliverable acceptance** for Fixed Price contracts, or monthly in arrears for T&M services.
Expenses	**Travel and subsistence expenses are included in the day rate / Billed at cost and in line with HMT guidance dependent upon contract terms**