

Service Definition Document

Cloud Architecture, AI & Data Analytics Design Consultancy for Public Sector, CNI and Sensitive Data (G-Cloud 15 – Lot 3: Cloud Support)

Supplier: IGUANA Ltd

Service Name: Cloud Architecture, AI & Data Analytics Design Consultancy

Service Category: Cloud Support (Architecture, Design and Assurance)

Service Version: v1.1

Last Updated: 18 January 2026

1. Service Overview

This service supports public sector and regulated organisations to design, modernise and assure secure cloud solutions for Critical National Infrastructure (CNI), mission-critical applications, and sensitive data environments. IGUANA provides end-to-end architecture and design consultancy spanning cloud foundations, application modernisation, data platforms and analytics, and AI/ML (including agentic AI) enablement. The service helps clients adopt scalable, resilient and compliant patterns across AWS, Azure and Google Cloud, while accelerating digital transformation and improving operational effectiveness.

2. Who the Service Is For

This service is intended for organisations that need secure, compliant and resilient cloud, data and AI designs, including:

- UK public sector bodies and ALBs
- CNI operators and critical service providers
- Regulated organisations (e.g., financial services, health, utilities)
- Teams handling sensitive or high-impact data workloads
- Programmes modernising legacy or critical applications
- Organisations implementing analytics, AI/ML, and automation capabilities

3. What the Service Includes

IGUANA can provide the following activities as part of the service:

3.1 Architecture Strategy and Planning

- Current-state assessment and architecture discovery
- Target-state architecture and transition roadmaps
- Architecture principles, standards and reference patterns
- Options analysis and technology selection support

3.2 Solution Architecture and Technical Modernisation

- Solution architecture and end-to-end design
- High-Level Design (HLD) and Low-Level Design (LLD)
- Application modernisation architecture (rehost, refactor, replatform)
- Microservices, API and event-driven architecture patterns
- Platform engineering patterns (self-service, automation, golden paths)

3.3 Cloud Foundations and Landing Zones

- Landing zone blueprint design
- Identity and access management design (federation, RBAC)
- Network architecture and segmentation (Zero Trust patterns)
- Shared services design (logging, monitoring, DNS, certificates)

3.4 Data Platforms and Analytics Architecture

- Data strategy, architecture and operating model alignment
- Data platform design (lakehouse, warehouse, streaming, batch)
- Data ingestion, integration and orchestration patterns
- Data governance, metadata, lineage and quality controls
- Analytics enablement (dashboards, KPIs, regulatory reporting)

3.5 AI/ML and Agentic AI Architecture Enablement

- AI/ML solution architecture and platform design (MLOps patterns)
- Model deployment patterns, monitoring and lifecycle management
- Responsible AI design (controls, traceability and governance alignment)
- Retrieval-Augmented Generation (RAG) architecture for secure knowledge access
- Agentic AI patterns (orchestration, tool use, guardrails, auditing)
- Automation of operational tasks using AI-enabled workflows

3.6 Security, Privacy and Sensitive Data Controls

- Data classification and protection controls
- Encryption, key management and secrets management design
- Secure architecture for sensitive workloads and critical services
- Security control mapping and evidence approach for assurance

3.7 Operational Resilience for Critical Services

- High availability and failover design
- Backup, restore and disaster recovery architecture
- Non-functional requirements design (performance, scale, reliability)
- Observability design (monitoring, logging, alerting)

3.8 Delivery Assurance and Governance

- Architecture governance, decision logs and traceability
- Design reviews, assurance checkpoints and sign-off support
- Alignment with programme delivery, Agile and DevSecOps practices
- Technical risk management and mitigation planning

4. Service Features

- Cloud architecture strategy, roadmaps and target-state definition
- Secure system design and architecture assurance for critical services
- Cloud landing zone design: network, identity, security baselines
- Sensitive data handling: classification, encryption, key management controls
- CNI-ready resilience: high availability, backup and disaster recovery design

- Data platform and analytics architecture for scalable insight delivery
- AI/ML and agentic AI architecture with guardrails and auditability
- DevSecOps and Infrastructure as Code design and governance
- Application and platform modernisation for legacy critical systems
- Vendor selection support with technical evaluation and due diligence

5. Service Benefits

- Reduces security risk for CNI and sensitive data workloads
- Improves resilience and uptime for critical public services
- Accelerates modernisation of legacy applications and platforms
- Enables faster analytics delivery through reusable data patterns
- Improves data quality, lineage and governance for trusted insights
- Speeds deployments using DevSecOps and Infrastructure as Code
- Reduces operational incidents via reliability engineering and assurance
- Enables safe AI adoption with guardrails, oversight and traceability
- Improves decision-making through actionable dashboards and analytics
- Lowers cloud costs through optimisation, governance and FinOps practices

6. Deliverables

Deliverables are agreed per engagement and may include:

- Architecture strategy and roadmap documents
- Target architecture and logical/physical designs
- HLD and LLD packs
- Landing zone blueprint and control baselines
- Application modernisation options and migration architecture
- Data platform architecture (ingestion, governance, analytics layers)
- AI/ML and agentic AI reference architectures and control patterns
- Resilience design (HA/DR/backup and restore approach)
- Security architecture artefacts and control mapping
- Architecture decision records (ADRs) and standards
- Delivery assurance reports and recommendations

7. Service Constraints and Dependencies

7.1 Constraints

- Delivery is primarily remote, with on-site support available by agreement.
- Access to secure environments (e.g., OFFICIAL-SENSITIVE) requires onboarding approvals.
- Work involving classified data may require additional controls and constraints.
- AI usage must comply with buyer policies for data handling and assurance.
- Implementation support is advisory unless delivery scope is explicitly agreed.

7.2 Dependencies

- Buyer provides timely access to stakeholders for workshops and decisions.
- Buyer provides necessary accounts, permissions, and technical environment access.
- Buyer provides current documentation, requirements, and known constraints.

- Delivery may be affected by governance approvals and accreditation timelines.

8. Support Model

8.1 Support Channels

- Email support
- Online ticketing support (request logging and tracking)
- Scheduled calls (as agreed)

8.2 Response Times

- Mon–Fri, 09:00–17:30 (UK time): Response within 4 business hours
- Weekends/UK bank holidays: Response within 1 business day (next working day)

8.3 Support Levels and Cost Approach

Standard Support (Included)

- Included during active consultancy delivery, email + ticketing support

Enhanced Support (Chargeable)

- Priority response and expanded coverage; charged on time-and-materials or retainer

Premium / CNI-Critical Support (Chargeable)

- Extended hours or 24/7 by agreement; charged via retainer + call-off rates

8.4 Technical Roles

- Technical Account Manager (TAM): Available for Enhanced and Premium support
- Cloud Support Engineer / Architect: Available for all tiers
- Data/AI Architect Support: Available as part of consultancy scope (as agreed)

9. Security and Compliance Approach

IGUANA designs solutions with strong emphasis on:

- Identity and access controls (least privilege, separation of duties)
- Network segmentation and secure connectivity patterns
- Encryption in transit and at rest, with controlled key management
- Logging, monitoring and security event visibility
- Resilience and continuity patterns for critical services
- Data governance controls for sensitive and regulated datasets
- AI governance patterns (auditability, guardrails, oversight and traceability)
- Governance, decision recording and evidence for assurance activities

Any client-specific policies and standards are incorporated into deliverables.

10. Onboarding and Start-Up

Typical onboarding steps:

1. Kick-off meeting and scope confirmation
2. Access and tooling setup (as required)
3. Discovery workshops and current-state review
4. Architecture/design iterations and assurance checkpoints
5. Handover of deliverables and implementation guidance

11. Service Management

IGUANA uses agreed working practices such as:

- Regular progress checkpoints (weekly/fortnightly)
- Document version control and review cycles
- Risk, issue and dependency management
- Architecture decision recording and approvals support

12. Ordering and Billing

- Services are delivered on a call-off basis under G-Cloud.
- Pricing is provided as agreed day rates or fixed outcomes where appropriate.
- Billing is typically monthly in arrears, aligned to agreed milestones or timesheets.

13. Service Hours and Location

- Standard service hours: Mon–Fri, 09:00–17:30 (UK time)
- Delivery: Remote by default, on-site by agreement
- UK-wide delivery supported depending on customer location and requirements

14. Termination and Offboarding

At the end of an engagement, IGUANA provides:

- Final deliverables and handover pack
- Knowledge transfer sessions (as agreed)
- Documentation archive and decision log summary
- Offboarding aligned to buyer's access removal process

15. Accessibility Statement

This service definition document is written using clear language and structured headings. IGUANA can provide deliverables in accessible formats on request and will follow buyer accessibility requirements for documentation and reporting.

16. Contact

Supplier: IGUANA Ltd

Service: Cloud Architecture, AI & Data Analytics Design Consultancy

Support Contact: Provided during onboarding (email and ticketing)

Service Hours: Mon–Fri, 09:00–17:30 (UK time)