airelogic

Cloud Support Services

G Cloud 15

Contents

1. Executive Summary

We support the design, delivery and operation of some of the UK's most complex and critical cloud services. By combining deep public-sector and health domain experience with strong engineering capability, pragmatic enterprise architecture and an ethical, employee-owned delivery model, we help organisations adopt and operate cloud services safely, sustainably and at scale.

Aire Logic is an employee-owned, ethical, B-Corp certified digital transformation partner specialising in large-scale cloud advisory, architecture, migration, optimisation and managed services across the UK public sector. With over 18 years of experience delivering highly available national platforms, including NHS Spine, MESH, the National Booking Service (NBS), API Management (APIM), Primary Care Registration Management (PCRM), Data Services (DPS/DSA), NHS Login and Vaccinations Digital Services (VDS), as well as Trust-level cloud and EHR platforms for organisations such as Leeds Teaching Hospitals Trust and The Christie, we bring proven expertise in designing, delivering and operating secure, resilient, cloud-native and hybrid environments.

As an independent, vendor-neutral supplier, we prioritise ethical delivery, open standards and long-term capability uplift, ensuring Buyers retain control of their cloud services and can transition suppliers or operate in-house where required.

This unified G-Cloud 15 service provides end-to-end cloud support, including:

- Cloud advisory & enterprise architecture
- Cloud migration planning & delivery
- Managed public, private and hybrid cloud
- Application management
- Cloud financial management (FinOps)
- Cloud environmental optimisation (GreenOps)
- Security strategy, design, risk, audit & incident response
- Quality Assurance, test automation & performance testing
- Ongoing support & service desk operations

All services described are **cloud-related and in full alignment with the G-Cloud 15 Lot 3 Cloud Support Services scope**.

2. Service Overview

We offer services that cover full lifecycle cloud support. These can be procured independently or as a complete service delivery package:

Plan: Cloud strategy, capability assessment, EA, options appraisal
Build: Cloud set-up, application modernisation, data migration, integration
Secure: Security architecture, risk assessment, incident response, audit
Test: Automation, functional, non-functional, performance testing
Run: Managed cloud, SRE, DevSecOps, 24×7 service desk
Optimise: FinOps, GreenOps, service optimisation, continuous improvement

We work in line with the **Government Digital Service (GDS) Service Standard**, **Open Standards Principles**, **NCSC Cloud Security Principles**, and UK public-sector **accessibility requirements (WCAG 2.2 AA)**.

We use open standards and portable cloud architectures to avoid vendor lock-in, enabling Buyers to transition to another supplier or in-house team at any time.

3. Full Service Scope (aligned to G-Cloud 15 Lot 3 Service Lines)

3.1 Managed Cloud Services (F-201)

We provide managed cloud services across public, private, and hybrid environments to ensure secure, reliable and optimised operation of cloud platforms throughout their lifecycle. Services can be delivered independently or as part of a wider cloud support engagement.

3.1.1 Managed Private Cloud

We deliver managed private cloud services covering IaaS, PaaS and application layers. This includes patching, monitoring, vulnerability remediation, configuration management and optimisation of private cloud environments.

We also provide administration of private PaaS and SaaS platforms, including databases, integration platforms and identity services, alongside application management covering deployments, configuration, observability and multi-tier (1st–3rd line) support. Backup, disaster recovery and restoration testing are provided in line with buyer continuity

requirements.

3.1.2 Managed Public Cloud (AWS, Azure, GCP)

We manage public cloud environments across AWS, Azure and GCP using Infrastructure as Code approaches, including Terraform, Bicep and CloudFormation. Services include management of serverless workloads, managed databases, messaging services and identity components.

Our cloud-native SRE services focus on resilience engineering, autoscaling, observability dashboards and proactive monitoring. Where required, services can be delivered with 24×7 operational support aligned to agreed service levels.

3.1.3 Managed Hybrid Cloud

We support hybrid cloud environments integrating public cloud, private cloud and on-premise systems. This includes hybrid identity and secure networking using VPN, Direct Connect and ExpressRoute, as well as interoperability between cloud and legacy platforms.

We also support legacy workload modernisation while maintaining hybrid operational stability, enabling gradual migration without service disruption.

3.2 Cloud Financial Management & GreenOps (F-202)

3.2 Cloud Financial Management & GreenOps (F-202)

We provide cloud financial management (FinOps) and sustainability-focused GreenOps services to help buyers optimise cost, performance and environmental impact across cloud platforms.

3.2.1 FinOps Services

Our FinOps services support transparent financial governance through cost allocation and tagging strategies, right-sizing analysis and workload efficiency reviews. We provide forecasting, budgeting and cloud spend modelling to support financial planning and decision-making.

Services also include Reserved Instance and Savings Plan optimisation, alongside FinOps dashboards, KPIs and governance processes to support ongoing cost control and capability uplift.

3.2.2 GreenOps Services

Our GreenOps services help buyers measure and reduce the environmental impact of cloud services through carbon footprint analysis, and sustainability reporting based on cloud usage data.

We apply energy-efficient architectural approaches such as serverless, autoscaling and event-driven design, alongside data lifecycle optimisation including intelligent tiering and archiving. We also provide recommendations aligned to low-carbon cloud regions and green procurement objectives.

Further details on our GreenOps approach and organisational sustainability practices are provided in **Section 13.1**.

3.3 Cloud Migration Planning (F-203)

3.3 Cloud Migration Planning

We provide structured cloud migration planning services to assess organisational readiness, define target-state architectures, and establish clear, achievable migration roadmaps aligned with buyer objectives, constraints, and governance requirements.

3.3.1 Capability Analysis

We assess organisational cloud readiness across people, process and technology, including current-state maturity, skills and team capability, and operational readiness for cloud adoption. This includes reviewing governance, support models, service management, and existing delivery practices to identify risks and capability gaps before migration.

3.3.2 Enterprise Architecture

We apply our EA Light methodology to define pragmatic, TOGAF-aligned target architectures and cloud operating models. This includes architectural principles, reference patterns, roadmaps and C4 modelling to clearly communicate cloud, integration and data designs across technical and non-technical stakeholders.

3.3.3 Cloud Gap Assessment

We conduct structured gap assessments across applications, data, infrastructure and security, including dependency mapping, technical debt analysis and compliance

considerations. Findings are documented with prioritised remediation actions to reduce migration risk and inform delivery planning.

3.3.4 Architecture Options Analysis

We evaluate public, private and hybrid cloud options using the 7Rs migration framework, considering cost, risk, performance and operational trade-offs. Architectures are designed for interoperability using open standards such as FHIR, SNOMED and HL7, ensuring portability and alignment with NHS and public-sector requirements.

3.3.5 Delivery Roadmapping

We produce sequenced migration roadmaps that prioritise workloads into achievable waves, aligned to business criticality and dependency constraints. Roadmaps also include skills uplift requirements and definition of the target end-state operating model to support sustainable live service operation.

3.4 Setup & Migration Delivery (F-204)

3.4 Set-Up & Migration Delivery

We deliver hands-on migration and setup services covering data, platforms, applications and operating models, working collaboratively with buyers and other suppliers to ensure safe transition to cloud environments.

3.4.1 Data Auditing & Organising

We perform data quality analysis, profiling and cleansing to understand the structure, volume and sensitivity of data prior to migration. This includes alignment of metadata, permissions and retention requirements to support secure and compliant cloud operation.

3.4.2 Data / Information Structure Design

We design cloud-ready data models, schemas and lineage, supporting master data management and API-based data flows. Designs consider scalability, interoperability and future analytics requirements.

3.4.3 Engagement & Communication Planning

We support stakeholder engagement through structured communication planning, including stakeholder mapping, user impact analysis and go-live communications to

minimise disruption during migration and transition activities.

3.4.4 Project Management & Governance

We provide PMO services including RAID management, delivery governance, status reporting and dashboards. This supports coordination across multi-disciplinary and multi-supplier teams and ensures progress, risks and decisions are visible and controlled.

3.4.5 Service Optimisation & Right-Sizing

We undertake performance tuning and resource optimisation activities before and after migration, including evaluation of cloud-native replacement options to improve efficiency, resilience and cost-effectiveness.

3.4.6 Mobilisation Coordination

We coordinate mobilisation activities across delivery teams, supporting cloud readiness uplift and early life support planning to ensure a controlled transition into live service.

3.5 Security Services (F-205)

3.5 Security Services

We provide cloud security services covering strategy, design, risk management, incident response, audit and security testing. Services are aligned to NCSC Cloud Security Principles and relevant public-sector and NHS security requirements.

3.5.1 Security Strategy

We define cloud security operating models and governance frameworks aligned to NCSC guidance and buyer risk appetite. This includes application of Zero Trust principles across cloud and hybrid environments to support secure access, data protection and operational resilience.

3.5.2 Security Risk Management

We provide structured security risk management services, including threat modelling and development of security risk registers. Risks are assessed, prioritised and supported with remediation planning to reduce exposure throughout the service lifecycle.

3.5.3 Security Design

We design secure cloud architectures covering identity and access management, encryption for data in transit and at rest, secure networking and API security. Controls include the use of WAFs, segmentation and cloud-native security services appropriate to the service risk profile.

3.5.4 Security Incident Management

We support preparation for and response to security incidents through documented incident response plans, runbooks and escalation paths. Where required, services can include optional 24×7 triage integrated with wider cloud support and service management processes.

3.5.5 Security Audit Services

We provide security posture reviews, cloud configuration audits and compliance assessments aligned to standards such as ISO 27001, Cyber Essentials Plus and the NHS DSP Toolkit. Findings are documented with clear recommendations to support remediation and assurance activities.

3.5.6 Security Testing

We support security testing through CI/CD-integrated automated testing, including SAST, DAST and dependency scanning, alongside remediation support for penetration test findings. This helps identify and address vulnerabilities early and continuously.

3.6 Quality Assurance & Performance Testing (F-206)

3.6 Quality Assurance & Performance Testing

We provide quality assurance and performance testing services to ensure cloud services are reliable, scalable, secure and fit for purpose. Services support both migration programmes and live service operations.

3.6.1 Test Automation

We deliver automated functional, API, UI and regression testing integrated into CI/CD pipelines. Automation improves test coverage, reduces manual effort and supports frequent, reliable releases.

3.6.2 Performance Testing

We undertake performance testing across cloud workloads, including load, stress, soak and scalability testing. Testing identifies bottlenecks and capacity limits to support resilient and predictable service performance.

3.6.3 Assurance & Test Design

We design test strategies aligned to the GDS Service Standard and NHS testing frameworks. This ensures testing approaches are proportionate, traceable and aligned to service and user needs.

3.6.4 Infrastructure Performance Testing

We benchmark cloud infrastructure components, including compute, storage, network and latency. Results inform optimisation, right-sizing and resilience decisions.

3.6.5 Operational Readiness Testing

We validate operational readiness through DR and failover testing, deployment readiness checks, monitoring validation and service desk readiness assessments. This supports a safe transition into live service.

3.6.6 Accessibility Testing

We provide accessibility testing to validate compliance with WCAG 2.2 AA and inclusive design requirements, supporting accessible digital services for all users.

3.7 Training Services (F-207)

We provide training services to support effective adoption, operation and optimisation of cloud services. Training is tailored to buyer roles and aligned to the required training outcomes.

3.7.1 Basic User Training

Basic user training supports end users in understanding and using cloud-enabled services as part of their day-to-day activities. Training focuses on core service functionality, standard workflows and user responsibilities within the service.

3.7.2 Super-User Training

Super-user training is designed for advanced users and administrators responsible for managing or configuring cloud services. Training covers administrative tasks, service configuration and operational responsibilities relevant to the buyer's environment.

3.7.3 Basic Troubleshooting Training

Basic troubleshooting training supports users and support staff in identifying and resolving common service issues. Training focuses on standard fault scenarios, initial diagnostics and escalation processes.

3.7.4 Advanced Troubleshooting Training

Advanced troubleshooting training is aimed at technical and support teams responsible for complex issue resolution. Training covers deeper diagnostic techniques, investigation of underlying causes and interaction with specialist support and engineering teams.

3.7.5 Function / Service Optimisation Skills

Optimisation training focuses on improving the performance, cost efficiency and sustainability of cloud services. This includes guidance on service tuning, efficient use of cloud resources and application of continuous improvement practices.

3.7.6 Other Training

Where required, we provide additional training tailored to buyer needs, such as onboarding new users, refresher sessions or role-specific training aligned to the services in scope.

Training is supported by guides, documentation, walkthroughs and refresher sessions to reinforce learning and support knowledge retention.

3.8 Ongoing Support Services (F-208)

We provide ongoing cloud support services to ensure stable, reliable and secure operation of cloud platforms following transition to live service.

3.8.1 Product Support Capabilities

We provide multi-tier (1st–3rd line) support for applications, APIs, data flows and cloud platforms. This ensures effective day-to-day operation and access to specialist support where required.

3.8.2 Logging and Management of Incidents

We manage incidents through structured logging, triage, resolution and root cause analysis. Trend analysis is used to identify recurring issues and support preventative improvement actions.

3.8.3 Reporting and Proactive Results Analysis

We provide continuous monitoring, alerting and proactive analysis using observability dashboards. Regular reporting covers incidents, service performance metrics, and insights from FinOps and GreenOps activities.

3.8.4 Dispatch of Service Technicians and/or Parts

Where applicable, we coordinate technician dispatch and replacement parts for hybrid or hardware-specific environments, working with buyers and third parties as required.

3.8.5 End-User Training Coordination

We coordinate end-user training activities, including knowledge transfer and documentation updates, to support effective service operation and continuous capability uplift.

3.9 Shared Responsibility Model

We work with Buyers to define clear boundaries of responsibility between the Buyer, us and the cloud provider. This includes responsibilities across security controls, incident response, governance, change management, data handling, operational processes and service continuity. This ensures all parties understand their roles within the cloud operating model and enables safe, compliant and effective cloud adoption.

4. Methodology & Delivery Approach

Our delivery methodology integrates enterprise architecture (including our EA Light approach), cloud adoption frameworks, DevSecOps and Site Reliability Engineering (SRE),

secure-by-design engineering, and quality assurance and testing disciplines. This holistic approach ensures that advisory, migration, managed services, security, testing and ongoing support are delivered consistently across the full service lifecycle.

This approach has been used to support delivery across large-scale and national programmes, including NHS Spine, MESH, the National Booking Service (NBS), API Management (APIM), Primary Care Registration Management (PCRM), Data Services (DPS/DSA), NHS Login and Vaccinations Digital Services (VDS), as well as regional and Trust-level cloud platforms.

4.1 EA Light – Agile Enterprise Architecture

EA Light is our pragmatic, lightweight, decision-focused approach that accelerates architecture without sacrificing governance. It is designed specifically for complex public-sector environments where technology, users, policy and suppliers must align quickly.

Core elements:

- Lightweight TOGAF-aligned architectural modelling
- C4 diagrams for clear solution visualisation
- Architectural principles & decision logs
- Cloud strategy & cloud operating model design
- Security architecture and data protection woven directly into designs
- Alignment with NHS and government standards (GDS, Tech Code of Practice, UK Gov Architecture Framework)

Used successfully on:

- **NHS Spine Core & Clinicals transformation** - enabling safe migration to cloud-native microservices.
- **NHS API Management (APIM)** - defining API-first architecture across a large multi-team delivery environment.
- **NHS National Booking Service** - designing a highly scalable Azure architecture used during periods of extreme national demand.

We have also demonstrated the use of AI to support engineering and service delivery across programmes such as the Electronic Prescribing Service and NHS Vaccinations Digital Services, improving onboarding efficiency and analytical insight by rapidly mapping business capabilities to existing systems and architectural decisions, enabling new teams

to understand complex environments quickly and make informed, traceable design decisions.

4.2 Cloud Adoption & Migration Framework

Our migration approach aligns with industry-leading models (Azure CAF, AWS Cloud Adoption Framework, Google CCAI) and incorporates our NHS-hardened delivery experience.

Phase 1 - Discovery & Assessment

- Current-state architecture
- Data discovery, profiling and lineage
- Security posture assessment (IAM, network, encryption, misconfiguration)
- Testing readiness & non-functional requirements (NFRs)
- Support & operational maturity assessment

Phase 2 - Target State Architecture

- Cloud-native vs hybrid vs private cloud patterns
- Microservices, APIs, event-driven architecture
- Identity & access architecture (SSO/Federation)
- Security design (WAF, segmentation, zero trust)
- High-level test approach (functional, non-functional, automation)

Phase 3 - Migration Planning

- 7Rs migration model
- Sequencing workloads into waves
- Replatforming/refactoring plans
- QAT environments & test data strategy
- Security accreditation planning
- Operational acceptance criteria

Phase 4 - Delivery & Implementation

- Infrastructure as Code (Terraform/Azure/Bicep/CloudFormation)
- CI/CD pipelines
- Application migration and cloud-native rebuilds
- Performance, load, and scalability testing
- Security testing (DAST/SAST)

Phase 5 - Transition to Live

- Operational Readiness Testing (ORT)
- Security sign-off
- Hypercare support
- DR/failover testing
- Support model handover

Phase 6 - Continuous Improvement

- FinOps optimisation
- GreenOps carbon improvement
- Security posture hardening
- Test automation expansion
- Technical debt reduction

4.3 DevSecOps & SRE Operating Model

We are recognised for delivering **DevSecOps at a national scale** for mission-critical cloud services, consistently meeting high reliability and 99.999% availability SLAs.

Core capabilities:

- CI/CD automation (GitHub Actions, Jenkins, ADO)
- Infrastructure as Code (IaC)
- Observability and monitoring (CloudWatch, App Insights, Grafana, Splunk)
- SRE practices: error budgets, reliability targets
- Security testing integrated into pipelines (SAST/DAST/OSS scanning)
- Automated test frameworks (integration, API, load, contract tests)

SRE pillars we implement:

- Availability targets & error budgets
- Automated alerting & dashboards
- Incident response & on-call
- Root cause analysis & blameless postmortems
- Deploy pipelines with automated quality gates
- Chaos testing / DR rehearsal (where appropriate)

4.4 Security-by-Design Approach

Our DevSecOps approach ensures security is integrated throughout:

- Threat modelling early in design
- Cloud provider best practice controls (AWS/CIS, Azure Security Benchmark)
- Secure coding standards (OWASP/CWE/CERT)
- CI/CD security testing (SAST/DAST)
- Encryption, key rotation, secrets management
- Security incident runbooks for managed services

This reduces vulnerabilities, strengthens compliance, and accelerates accreditation.

4.5 Testing & Quality Assurance Approach (QAT)

We provide a comprehensive and unified model for functional, non-functional and performance testing:

Test Strategy & Planning

- End-to-end test approach across migration phases
- Environment design for realistic workloads
- Data anonymisation, synthetic data creation

Test Automation

- API automation
- UI automation
- Contract testing
- Regression packs

Performance & Load Testing

- Load, stress, soak and scalability testing
- Bottleneck analysis (network, API, compute, database)
- Cloud cost-aware testing (avoiding unnecessary resource use)

Operational Readiness Testing

- DR/failover testing
- Service desk readiness
- Monitoring and alerting validation
- Security incident simulation

5. Case Studies

We have extensive experience supporting national and regional public-sector digital services, delivering cloud engineering, architecture, data, security, quality assurance, AI enablement and operational support at scale. The following examples illustrate how approaches such as EA Light, DevSecOps/SRE, secure-by-design engineering and service optimisation have been applied in practice.

5.1 National Booking Service (NBS) - Azure Cloud, High-Volume Platform

The National Booking Service enables vaccination and healthcare bookings across the UK. We led the architecture, engineering, DevSecOps, quality assurance and operational support across several phases of the service's evolution.

Highlights:

- Supports **1M+ bookings per day** during peak demand
- Azure Front Door routing, autoscaling and global resilience
- Test automation and performance testing to prepare for new seasonal demand
- Secure integration with the NHS App (~32 million users)
- 24×7 on-call availability during vaccination campaigns

We also contributed to the national multi-supplier delivery model, working across product, architecture, DevSecOps, data and assurance teams to deliver rapid, policy-driven improvements to digital vaccination services.

To complement this work, we delivered AI-enabled tooling used across NHS digital services, including onboarding support that reduces manual workload and improves service responsiveness.

5.2 Spine & Spine Futures - National Integration Platform

We contributed architecture, engineering, security and quality assurance expertise to the NHS Spine and Spine Futures programmes, supporting the evolution towards cloud-native, event-driven microservices on AWS.

Highlights:

- Migration of key components into AWS microservices
- Supports 99.999% uptime and approximately 1.3bn messages per month
- Security-by-design, including IAM, WAF, encryption and load balancing
- Automated security scanning integrated into CI/CD
- Performance engineering and contract testing for critical national workloads
- 24×7 platinum live service support

Our EA Light methodology supports faster architectural decision-making across complex, multi-supplier delivery teams, while maintaining governance and assurance appropriate for a national platform.

5.3 MESH to Cloud - Secure Serverless Architecture

We supported the secure, event-driven cloud migration of the national MESH (Message Exchange for Social Care and Health) service to AWS, enabling more resilient and scalable handling of high-volume file transfers.

Highlights:

- Serverless architecture using Lambda, DynamoDB, SQS/SNS
- Continuous security scanning and strong IAM controls
- Event-driven automated testing integrated into CI/CD
- FinOps optimisation to improve cost efficiency
- Rapid incident response and operational support

This work strengthened the resilience, observability and maintainability of a critical national messaging service.

5.4 Data Service Alliance (DSA) - Cloud Data Pipelines

We contributed to the design, engineering and assurance of secure cloud data pipelines supporting multiple national datasets across health, mental health and community services.

Highlights:

- Secure ingestion, transformation and delivery of national datasets
- Scaled COVID-19 laboratory data pipelines to **10 million tests per day**
- CI/CD pipelines for data transformations and quality checks
- Load and performance testing of very large data flows

- Integrated 3rd-line support and incident response

We have also supported secure analytics environments handling **200+ sensitive datasets** and **190+ access profiles**, applying strong governance and NCSC-aligned security patterns.

5.5 PPM+ EHR Cloud Migration – Leeds Teaching Hospitals

We supported Leeds Teaching Hospitals in the cloud migration and modernisation of their PPM+ Electronic Health Record (EHR) platform, including hybrid cloud integration, QAT, sustainability improvements and operational support.

Highlights:

- Migration of major EHR components containing **7m+ patient records**
- Hybrid cloud architecture integrating on-premise systems with cloud-native services
- Quality assurance for clinical safety and performance
- **GreenOps improvements**, including architectural changes that **significantly reduced CO_2e consumption**
- Scalable services capable of processing **millions of documents per month**
- 24×7 support wrap during critical transition periods

We also delivered structured capability uplift programmes, including Automation 101, enabling testing and engineering teams to increase automation coverage and accelerate delivery.

5.6 Additional AI Capability Supporting National Cloud Services

In addition to our core cloud advisory, migration, managed services, security and assurance capabilities, we are at the forefront of applying AI capabilities within national, cloud-based public sector services to improve efficiency, insight and service operation.

For the NHS Electronic Prescription Service (EPS), we developed an AI-enabled onboarding and support chatbot trained on complex technical guidance. This capability is used by approximately 40% of EPS suppliers, reducing manual support effort and improving onboarding consistency.

We also supported the delivery and operational readiness of an AI-based anomaly detection proof-of-concept for the NHS Vaccinations Programme. While deployment was paused due to data authorisation constraints, the work is informing analytics and assurance activities on other national platforms.

5.8 Leeds City Council – Skills Analysis and Digital Competency Framework

We conducted a digital skills analysis across 185 council staff, resulting in a competency framework and training roadmap aligned to the Council's cloud and digital transformation strategy. This work enabled targeted upskilling and organisational readiness for future digital capability requirements.

6. Onboarding

Our onboarding process ensures rapid mobilisation while maintaining governance. All activities below will be managed by a dedicated Aire Logic Mobilisation Manager.

6.1 Onboarding Activities

- Kick-off workshops & requirement confirmation
- Access provisioning & security checks
- Cloud environment setup (where in-scope)
- Review of existing architecture, workloads and SLAs
- Migration or management plan finalisation
- Dashboard and reporting setup (FinOps, SRE, sustainability)
- Contract-specific KPIs and success criteria

6.2 Onboarding Timeframes

Onboarding timelines vary depending on the Buyer's requirements, service complexity and the scale of existing systems and integrations.

Typical onboarding takes approximately 2–6 weeks, but we will work collaboratively with the Buyer during mobilisation to define a tailored onboarding plan and schedule. This will ensure a controlled transition, minimal disruption to services and clear alignment of expectations from the outset.

7. Offboarding

We ensure a clean, safe and compliant offboarding process aligned with G-Cloud requirements. We aim to leave the Buyer with everything required to operate, maintain and evolve their cloud services independently, with confidence and without disruption.

7.1 Offboarding Activities

Offboarding activities typically include:

- Data export or transfer in line with buyer requirements
- Asset, documentation and architecture artefact handover
- Handover of runbooks, patterns and operational knowledge
- Structured knowledge transfer sessions with buyer teams and/or incoming suppliers
- Removal of security access and credentials
- Transfer of monitoring, alerting and operational dashboards
- Supplier transition support, including shadowing where required
- Exit report documenting service improvements, known risks and recommended next steps

7.2 Offboarding Timeframes

Offboarding timelines depend on the Buyer's environment, the services in scope and the complexity of data, integrations and operational dependencies.

Typically, offboarding takes 2–4 weeks unless large data migrations are required.

We will work collaboratively with the Buyer at call-off to define a tailored offboarding plan and schedule. This will ensure continuity of operations, a controlled transition to alternative suppliers or internal teams, and full documentation and knowledge transfer to support ongoing service stability.

7.3 Avoidance of Lock-In

We avoid supplier lock-in through open standards (FHIR, REST, SNOMED, HL7), portable cloud architectures, Infrastructure-as-Code, comprehensive documentation and full offboarding support. Buyers retain full control of their data, configuration and environments, and can transition to another supplier or in-house team (with our support)

at any time.

8. Service Levels (SLAs)

We provide flexible, buyer-specific SLAs aligned to the criticality of the cloud services we support. SLAs are defined during onboarding and can be adapted for public cloud, private cloud, hybrid cloud, security services, testing and operational support.

8.1 Incident Response Times

Incident response and resolution times will be confirmed with the Buyer at call-off and tailored to the criticality, service hours and support model required. We typically operate a priority-based incident management model aligned to ITIL practices, as outlined below.

Priority 1 – Critical Service Outage

- Typical response time: **15 minutes**
- Typical resolution target: **4 hours**
- 24×7×365 optional coverage
- Evidenced across national services such as Spine, MESH and NBS

Priority 2 – Major Service Degradation

- Typical response time: **30 minutes**
- Typical resolution target: **8 hours**
- Automated escalation to engineering & security teams

Priority 3 – Service Issue / Reduced Functionality

- Typical response time: **4 business hours**
- Typical resolution target: **2 working days**

Priority 4 – Minor Issue / General Support

- Typical response time: **1 working day**
- Typical resolution target: **5 working days**

We have delivered **Platinum 24×7×365 SLA operations** for major national platforms, including **Spine, MESH, APIM and NBS**, demonstrating our capability to support mission-critical environments.

8.2 Availability Examples

Standard Business-Critical Cloud Services

99.5–99.9% availability

High-Criticality Cloud Services

99.95% availability

National-Scale / Mission-Critical

99.999% availability (as achieved on NHS Spine)

8.3 Security Response SLAs

(For security incidents, integrated into Cloud Support services)

- Critical security incident triage: **15 minutes**
- Forensic analysis initiation: **1 hour**
- Containment actions: **2 hours**
- Detailed Root Cause Analysis (RCA): **Within 48 hours**

These SLAs reflect experience supporting AWS, Azure and hybrid security events across national-scale mission-critical systems.

8.4 QAT & Testing SLAs

- Test automation suite execution: **within CI/CD window**
- Performance test analysis report: **5–10 working days**
- Accessibility testing: **within the agreed sprint cycle**
- Regression test cycle: **within release cadence**

8.5 Monitoring & Reporting SLAs

- Proactive monitoring (24×7 optional)
- Dashboards refreshed in near-real time
- Monthly service reports (or weekly for high-criticality services), including:
    - Incident summaries
    - Root cause analyses
    - FinOps cost optimisation
    - GreenOps sustainability insights

- Test coverage, defects, and performance metrics
- Change log and release notes

9. Pricing Model

We offer multiple pricing options and will work with the Buyer to determine the most appropriate model for the effective delivery of their requirements. All pricing follows G-Cloud rules and uses simple, transparent models suitable for advisory, engineering, testing, security and ongoing support services.

9.1 Pricing Options

- **Time & Materials / Day Rates**
  - Architecture, advisory, security, testing, migration, DevSecOps, PMO
- **Fixed Price Packages (optional)**
  - Cloud readiness assessment
  - Application migration discovery
  - Security threat modelling
  - Performance/load testing packages
- **Managed Service Subscription**
  - Ongoing cloud support
  - Security monitoring
  - Application management
  - Incident handling
- **Blended Team Rates**
  - Multi-disciplinary teams (cloud, security, QAT, DevSecOps, data)
- **Outcome-Based Pricing (optional)**
  - By agreement for defined deliverables

Framework rates are available through the framework. Contact us for a pricing discussion.

All costs exclude VAT and comply with G-Cloud pricing transparency requirements.

10. Service Constraints

Service constraints depend on buyer environments and may include:

- Buyer must provide system access, VPNs, firewall changes or cloud tenancy admin rights
- Legacy systems may require extended testing or remediation before cloud migration
- Security clearance (BPSS/SC/NPPV) may affect onboarding speed and require sponsorship from the Buyer
- Penetration testing or audit windows controlled by external parties
- QAT activities require appropriate non-production test environments
- Multi-supplier ecosystems may impose coordination dependencies
- External licensing and proprietary systems may limit automation

Constraints will be identified early during mobilisation and onboarding to mitigate risk.

11. Dependencies

Dependencies vary per engagement and typically include:

11.1 Buyer-side Dependencies

- Access to SMEs and decision-makers
- Availability of documentation (architecture, integrations, configs)
- Access to cloud tenancy (AWS/Azure/GCP) for setup activities
- Access to test data, API documentation and existing pipelines
- Alignment with buyer governance and release processes

11.2 Third-Party Dependencies

- APIs or systems owned by other suppliers
- External security testing availability
- Network or infrastructure changes managed by other vendors

11.3 Cloud Provider Dependencies

- Availability of specific cloud services in required regions
- Provider-side maintenance or outages

Dependencies will be logged, managed and tracked through the programme RAID process. Dependencies will be identified early during discovery and mobilisation to mitigate delivery, operational and integration risks.

12. Buyer Responsibilities

To ensure smooth delivery, buyers are typically responsible for:

- Providing timely access to systems, environments, networks and documentation
- Maintaining governance and internal approvals for architecture, security and releases
- Ensuring access to credentials, cloud tenancy controls and IAM permissions
- Providing test data or agreeing on a synthetic data approach (for QAT)
- Ensuring on-site access for technician dispatch (where applicable)
- Managing third-party contracts and licences not included in this service
- Ensuring organisational readiness for support handover (service desk, comms, training)

Buyer responsibilities will be confirmed at the call-off stage.

13. Sustainability

We are a sustainability-driven organisation with environmental responsibility embedded across every aspect of our cloud advisory, engineering, migration, testing and support services.

We are:

- **B-Corp Certified** (Score 108.1)
- **ISO 14001 Certified** (Environmental Management)
- **ISO 26000 Aligned** (Social Responsibility)
- **Committed to Net Zero by 2030**
- A founding participant in **Leeds GreenTech** sustainability initiatives

Our Environmental Management Representative and Green Working Group ensure sustainability is reflected both in our internal operations and the cloud solutions we

design for customers.

13.1 GreenOps - Sustainability Built into Cloud Operations

Our GreenOps practice supports organisations to measure, manage and reduce the carbon footprint of cloud services through:

Energy-Efficient Architecture

- Serverless-first designs
- Autoscaling to avoid idle compute
- Efficient event-driven patterns
- Reduction of heavy, long-running batch workloads

Carbon-Aware Deployment

- Use of cloud regions powered by renewable energy
- Resource right-sizing
- Cost + carbon trade-off modelling
- Improving utilisation efficiency during performance testing

Data Lifecycle Optimisation

- Minimising unnecessary data retention
- Optimised data storage tiers
- Intelligent archiving using cloud-native storage lifecycle rules

Environmentally Responsible DevSecOps

- Shorter build times
- Reduced pipeline compute waste
- Use of ephemeral / on-demand test environments

Example:

- **PPM+ EHR migration** significantly reduced CO_2e consumption by replatforming compute-intensive workloads to a more efficient cloud model while scaling to process millions of documents per month.

13.2 Organisational Environmental Initiatives

We go beyond cloud design with operational sustainability practices such as:

- 100% renewable electricity in all offices
- Investments in Ripple Energy solar and wind farms, offsetting 100% of predicted office emissions for 40+ years
- Annual carbon footprint mapping using internal analytics tools
- Company-wide environmental training
- Updated travel and procurement policies, reducing emissions
- Active staff-led **Green Working Group** governing environmental strategy

These commitments strengthen our ability to provide sustainable cloud advisory and managed cloud services.

14. Why Aire Logic

We offer a rare combination of cloud engineering excellence, enterprise architecture experience, public-sector insight, strong organisational ethics and proven delivery across some of the most complex digital ecosystems in the UK.

14.1 Proven Public-Sector and Health Domain Experience

For over 18 years, we have delivered cloud, data and digital platforms used at a national scale across health and the wider public sector. Our experience spans citizen-facing services, national integration platforms, secure data pipelines and Trust-level clinical systems, supporting programmes such as NHS Spine and Spine Futures, MESH, the National Booking Service, NHS Login and major EPR cloud migrations. This depth of domain understanding allows us to design and operate cloud services that are safe, resilient and aligned to public-sector governance and policy constraints.

14.2 Full-Stack, Multi-Cloud Capability

We provide end-to-end cloud expertise across AWS, Azure, GCP and hybrid environments, covering infrastructure, platforms, applications, security, data and integration. Our teams work across serverless, containerised and traditional cloud architectures, applying cloud-native services and Infrastructure as Code to deliver scalable, maintainable and portable solutions. This breadth is demonstrated across live services rather than

certifications alone (e.g. AWS, Azure and hybrid cloud delivery referenced throughout Section 5).

14.3 Mature DevSecOps, SRE and Quality Engineering

We operate some of the UK's most demanding digital services, applying mature DevSecOps, Site Reliability Engineering and quality assurance practices to support high availability, frequent releases and secure operation. Our approach integrates CI/CD automation, Infrastructure as Code, security testing, performance engineering and observability to deliver reliable, cost-effective cloud services at scale (e.g. national platforms such as Spine, MESH and the National Booking Service).

14.4 Ethical, Employee-Owned & B-Corp

As an employee-owned and B-Corp certified organisation, we are committed to ethical delivery, long-term public value and environmental responsibility. Our practices are underpinned by recognised standards including ISO 27001, ISO 14001, ISO 26000 and Cyber Essentials Plus. This governance and values-led approach aligns closely with public-sector priorities around transparency, sustainability and social value.

14.5 Scalable and Flexible Delivery

We operate a scalable delivery model with multi-disciplinary teams spanning architecture, engineering, security, testing, DevSecOps, data and delivery management. This allows us to mobilise rapidly and adapt capacity to meet changing demand, while maintaining delivery rigour and continuity. Buyers benefit from the agility of a product-focused organisation combined with the assurance expected of an enterprise delivery partner.

14.6 Vendor-Neutral and Standards-Based

We are vendor-neutral and do not resell technology products. We recommend and implement solutions based solely on buyer needs, using open standards and widely adopted frameworks to avoid lock-in and support long-term sustainability. Our work aligns with standards such as FHIR, SNOMED, HL7, the GDS Service Standard and NCSC Cloud Security Principles, ensuring interoperability, portability and ease of transition at exit.

15. Contact Details

Aire Logic Limited
Company Number: 06233174
Aireside House, 24-26 Aire Street, Leeds, LS1 4HT
https://airelogic.com/

G-Cloud Enquiries

Email: procurement@airelogic.com
Phone: 01134688527