Colibri Digital

# G-Cloud 15 Service Definition

## AWS Cloud-Native Modernisation

## with DevSecOps

# Contents

# 1. Service Overview

| | |
|---|---|
| **Supplier Name** | GCI NETWORK SOLUTIONS LIMITED |
| **Service Branding** | Colibri Digital |
| **Framework** | G-Cloud 15 (RM1557.15) |
| **Service Type** | Lot 3: Cloud Support |

Colibri Digital's AWS Cloud-Native Modernisation with DevSecOps service provides technical support and advisory expertise to assist organisations in transitioning legacy applications into high-performing, cloud-native solutions. We evaluate workloads using the 7 R's approach to identify the most effective modernisation path based on business value and technical constraints.

The service provides the technical design and guidance required to integrate DevSecOps principles, supporting the development of automated CI/CD pipelines and Infrastructure as Code (IaC) architectures. This ensures modernisation is aligned with NCSC 'secure-by-design' principles for OFFICIAL-SENSITIVE workloads.

**NOTE: This service definition covers time-bound professional services activities for assessment, design, and implementation. Ongoing managed operations and 24/7 support are out of scope.**

Key technical components of the delivery include:

| | |
|---|---|
| **Infrastructure as Code (IaC)** | Advisory on environment automation using Terraform/AWS Cloud Development Kit (AWS CDK) to support immutable and repeatable deployments. |
| **Advanced CI/CD Pipelines** | Technical guidance on high-frequency delivery toolsets featuring supporting deployment patterns such as Blue/Green or Canary, where appropriate. |
| **Observability & SRE** | Integration of Amazon CloudWatch, AWS X-Ray, and centralised logging in a dedicated security account to provide real-time visibility and an automated audit trail. |
| **The 7 R's Strategy** | A structured assessment framework to identify the most cost-effective modernisation path for unique workloads. |
| **API-First Design** | Decoupling legacy dependencies through Amazon API Gateway, enabling seamless integration with modern data platforms and third-party services. |
| **Automated Guardrails** | Configuration support for SCPs and AWS Config Rules to align with UK data sovereignty requirements. |

Core Public Sector use cases include:

| | |
|---|---|
| **Legacy Application Refactoring** | Transforming monolithic legacy applications into microservice architectures to improve scalability and maintainability. |

| | |
|---|---|
| **Automated Compliance & Security** | Implementing "Compliance as Code" within CI/CD pipelines to ensure every deployment meets NCSC Cloud Security Principles automatically. |
| **Rapid Digital Transformation** | Enabling departments to move from manual, error-prone releases to automated, high-frequency deployments using AWS CodePipeline and GitHub/GitLab. |
| **Cost Optimisation & Efficiency** | Re-platforming workloads to leverage serverless (AWS Lambda) or containerised (Amazon Fargate) technologies to reduce operational overhead and compute costs. |
| **Resilience Engineering** | Modernising applications to be multi-AZ and self-healing, ensuring critical public services remain available during infrastructure disruptions. |

## 2. Features & Benefits

The following table outlines the core technical features of the assessment and the specific value outcomes they provide to public sector organisations.

| | |
|---|---|
| **7 R's Assessment Framework** | **Strategic Alignment.** Identifies the optimal modernisation path to support ROI and technical feasibility. |
| **Infrastructure as Code (IaC)** | **Consistency & Speed.** Uses Terraform or AWS CDK to ensure environments are repeatable, version-controlled, support repeatable deployments, and reduce configuration drift. |
| **DevSecOps Pipelines** | **Risk Mitigation Support**. Identifies technical requirements for automated security scanning within pipelines. |
| **Containerisation & Serverless** | **Operational Efficiency.** Evaluates opportunities for serverless/containerised architectures to support team focus. |
| **Documentation** | **Knowledge Sovereignty.** Provides full handover of code and designs to facilitate independent management. |
| **NCSC Alignment** | **Streamlined Accreditation.** Built-in security controls simplify the process for Senior Information Risk Owners (SIROs) to approve live operations. |

## 3. Technical Requirements & Implementation

The service is delivered in line with the Government Digital Service (GDS) Service Standard, applying an iterative, evidence-led approach to reduce delivery risk and ensure services are secure, reliable, and user-focused.

Delivery follows a structured four-phase model, allowing customers to adopt the service incrementally and maintain control over scope, risk, and cost throughout implementation.

1. **Discovery**

The Discovery phase establishes a clear understanding of the customer's current technical environment and constraints. Activities typically include:

- Analysis of the existing architecture, platforms, and integrations
- Identification of technical debt and legacy dependencies
- Assessment of data classification, data residency, and sovereignty requirements
- Review of operational, security, and compliance constraints
- Definition of success criteria and high-level migration options

Outputs from Discovery are used to inform the recommended technical approach and reduce delivery risk before any migration activity begins.

2. **Alpha**

Validation of proposed solutions through a PoC to provide evidence of technical viability. The Alpha phase validates the proposed solution through a Proof of Concept (PoC). This is delivered in a sandboxed cloud environment to ensure no impact on live services. Typical activities include:

- Configuration of a representative cloud environment
- Validation of tooling, automation, and migration patterns
- Early security and access control configuration
- Testing of connectivity, performance, and integration assumptions

Alpha provides evidence that the proposed approach is technically viable and meets customer requirements before progressing to live workloads.

3. **Beta**

Technical support for pilot migrations, refining runbooks and monitoring processes based on findings. During Beta, the service supports a pilot migration of non-critical services, typically with limited live traffic. Activities include:

- Migration of agreed pilot workloads
- Controlled exposure to live users or traffic
- Performance, resilience, and operational testing
- Refinement of runbooks, monitoring, and support processes
- Validation of security controls in a live context

Beta allows customers to confirm operational readiness and build internal confidence before full-scale deployment.

4. **Live**

Transition & Stabilisation Support during the migration of production services. This includes mentoring staff, validating security guardrails, and delivering a structured knowledge

handover to the buyer's steady-state team. This phase includes:

- Execution of the agreed migration plan
- Cutover and validation activities
- Integration with live monitoring and support tooling
- 24/7 hyper-care support during the stabilisation period
- Handover to steady-state service management

Live delivery is designed to minimise disruption to end users and operational teams.

## 4. Security & Quality Assurance

We provide security assurance documentation and runbooks mapped to NCSC principles, as agreed. SC-cleared staff can be provided, subject to availability and buyer requirements.

| | |
|---|---|
| **Secure Development** | Modernised components use version-controlled IaC with automated linting to support code quality and consistency. |
| **Threat Detection** | Configuration support for AWS native security services (e.g., Amazon GuardDuty and AWS Security Hub) to provide visibility and automated alerts for potential security vulnerabilities. |
| **Data Protection** | Assistance in defining encryption-at-rest and in-transit strategies using AWS KMS and Certificate Manager to align with NCSC data protection requirements. |
| **Standards** | Our delivery processes are certified to ISO 27001 and Cyber Essentials Plus. |

## 5. Support & Service Levels

This service definition covers time-bound professional services activities for assessment, design, and implementation. Ongoing managed operations and 24/7 support are out of scope.

## 6. Constraints

The following constraints apply to the AWS Cloud-Native Modernisation with DevSecOps service to ensure transparency and prevent operational disputes:

| | |
|---|---|
| **Professional Services Scope** | This is a Lot 3 Cloud Support offering; it does not include the ongoing cost of AWS resource consumption or the provision of third-party software licences. |

| | |
|---|---|
| **Legacy System Compatibility** | While we specialise in modernising legacy workloads, the feasibility of refactoring is dependent on the availability of source code, expertise, and documentation for the existing monolithic systems. |
| **Network Infrastructure** | The speed and performance of modernised applications integrated with on-premises systems are constrained by the buyer's existing network infrastructure and bandwidth. |
| **Security Guardrails** | To maintain an NCSC-aligned security posture, certain core "guardrail" policies (Service Control Policies) cannot be disabled without a formal risk acceptance from the buyer. |
| **Identity Provider Integration** | Full automation of DevSecOps user management is dependent on the buyer's internal Identity Provider (e.g., Entra ID) supporting standard protocols such as SAML 2.0. |
| **Cloud Provider Availability** | Service availability is subject to the underlying AWS Service Level Agreements (SLAs) for the appropriate AWS region. |
| **Maintenance Windows** | Certain modernisation activities or platform updates may require scheduled maintenance windows, which will be agreed upon in advance to minimise disruption. |

## 7. Data Restoration & Disaster Recovery

Our service prioritises Resilience Engineering by identifying architectures that replace manual routines with automated, code-driven recovery patterns. We evaluate RTO and RPO requirements to recommend Infrastructure as Code (IaC) recovery blueprints. To support operational readiness, we assist in the validation of restoration plans to identify gaps in resilience before production use.

### Backup & Restore Approach

All modernised workloads are configured with automated backup policies integrated into the Infrastructure as Code (IaC) templates.

| | |
|---|---|
| **Automated Backups** | Leveraging AWS Backup to centralise and automate data protection across AWS services (EBS, RDS, Aurora, DynamoDB, EFS, and S3). |
| **Immutable Backups** | Utilising Amazon S3 Object Lock and AWS Backup Vault Lock to prevent accidental or malicious deletion, protecting against ransomware. |
| **Point-in-Time Recovery (PITR)** | Database workloads are configured with PITR enabled, allowing restoration to any specific second within the retention window. |
| **Cross-Region Copy** | For critical services, backups are automatically replicated from the primary |

AWS region to a secondary region to protect against regional outages.

## Disaster Recovery (DR) Strategies

We implement DR strategies tailored to the criticality of the specific workload, as defined during the 7 R's Assessment Framework phase:

| | |
|---|---|
| **Backup & Restore** | Data is backed up to S3; infrastructure is redeployed via Terraform or AWS CDK upon failure. |
| **Pilot Light** | Core data is mirrored; a minimal "scaled-down" version of the environment sits idle. |
| **Warm Standby** | A functional, scaled-down version of the full environment is always running in a second AZ. |
| **Multi-Site Active-Active** | Traffic is served from multiple Availability Zones (AZs) simultaneously with real-time replication. |

## Resilience Engineering & Validation

To ensure that "Data Restoration" is a proven capability rather than a theoretical plan, our service includes:

| | |
|---|---|
| **Infrastructure as Code (IaC) Recovery** | Since environments are defined in Terraform or AWS CDK, we can recreate entire application stacks from scratch in minutes if an environment becomes corrupted. |
| **Automated Recovery Testing** | We integrate restoration tests into the CI/CD pipeline to verify that backup snapshots are valid and bootable. |
| **Self-Healing Architectures** | Utilising AWS Auto Scaling and Health Checks to automatically detect and replace failing instances without manual intervention. |
| **Documentation** | As part of the Knowledge Sovereignty benefit, we provide comprehensive DR Playbooks and Runbooks, detailing the manual and automated steps required for failover and failback. |

## Business Continuity

Following NCSC Cloud Security Principle 9, we modernise monolithic systems into microservices to limit the impact - or "blast radius" - of individual component failures. This ensures a single module's downtime does not compromise the entire user experience. To support seamless continuity, staff can securely access these workloads from any location using Desktop as a Service (DaaS) or VPN solutions, supporting continuity design considerations, subject to the buyer's operating model and agreed controls.

# 8. Onboarding & Offboarding

## Onboarding
Scheduled following call-off, subject to buyer availability and mobilisation dependencies.

## Offboarding & Exit
We follow a structured exit process designed to eliminate supplier dependency. As all modernised components are defined via open-standard IaC (Terraform/CDK), the buyer retains full ownership of the configuration and code repositories.

## Data Portability
All documentation is handed over in open formats (pdf).

## Knowledge Handover
We provide technical briefing sessions and documentation to the buyer's internal teams. This ensures 'Knowledge Sovereignty,' allowing the buyer to manage, patch, and update the modernised applications independently after our access is revoked.