



Colibri  
Digital

G-CLOUD 15 SERVICE DEFINITION

**AWS WELL-ARCHITECTED**

**REVIEW**

## Contents

|                                                     |   |
|-----------------------------------------------------|---|
| 1. Service Overview                                 | 3 |
| 2. Features & Benefits                              | 4 |
| 3. Technical Requirements                           | 5 |
| 4. Security & Quality Assurance                     | 6 |
| 5. Support & Service Levels                         | 6 |
| 6. Constraints                                      | 6 |
| 7. Data Restoration & Disaster Recovery             | 6 |
| Our Approach to DR Planning                         | 6 |
| DR Strategy Mapping                                 | 7 |
| Technical Validation & Infrastructure as Code (IaC) | 7 |
| Shared Responsibility Model                         | 7 |
| 8. Onboarding & Offboarding                         | 8 |
| Onboarding                                          | 8 |
| Offboarding & Exit                                  | 8 |
| Data Portability                                    | 8 |
| Knowledge Handover                                  | 8 |

## 1. Service Overview

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

Our AWS Well-Architected Review provides evaluation of AWS workloads against the six core pillars of your AWS workloads across the six core pillars: Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimisation, and Sustainability. As a UK AWS MSP and Well-Architected Launch Partner, Colibri Digital extends the standard framework by applying experience-based insights and internally developed Secure-by-Design documentation to deliver an assessment that addresses the specific complexities of public sector cloud that addresses the specific complexities of public sector cloud environments.

The service focuses on two critical emerging disciplines: FinOps, to drive financial accountability and cost transparency, and GreenOps, to minimise the environmental footprint of your cloud operations through energy-efficient architecture. We don't just identify high-risk issues; we provide a prioritised remediation backlog that aligns with public sector governance and the GDS Service Standard.

Beyond the standard binary "pass/fail" check, our assessment examines FinOps maturity. This supports departments in tracking and justifying IT spend in line with central government budgetary requirements.

Furthermore, our GreenOps assessment methodology evaluates your workload's "Carbon Intensity". This enables public sector bodies to evidence progress toward Net Zero targets through tangible, data-backed AWS sustainability improvements.

Every review is underpinned by our Secure-by-Design philosophy, which maps architectural findings directly to the NCSC 14 Cloud Security Principles. We evaluate your use of AWS Control Tower, automated guardrails, and immutable logging to ensure that security is foundational to your operations rather than an afterthought. The final output is a delivery-ready backlog that provides Senior Information Risk Owners (SIROs) with documentation to support the accreditation process for OFFICIAL-SENSITIVE workloads.

**NOTE: This service definition covers time-bound professional services. Ongoing managed operations and 24/7 support are out of scope, unless agreed otherwise. Also, the review supports organisations in understanding alignment with AWS Well-Architected principles. It does not constitute certification or formal assurance.**

Core Public Sector use cases include:

|                                      |                                                                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FinOps Cost Recovery</b>          | Identification of wasted spend, underutilised resources, and commitment-based savings opportunities to maximise taxpayer value.           |
| <b>GreenOps Sustainability Audit</b> | Assessment of workload carbon impact and energy efficiency, providing actionable steps to align with departmental sustainability targets. |

|                                          |                                                                                                                                                                                                                                                                  |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NCSC Security Alignment</b>           | Review of the Security pillar mapped against the NCSC 14 Cloud Security Principles to support OFFICIAL-SENSITIVE accreditation.                                                                                                                                  |
| <b>Resilience &amp; DR Validation</b>    | Stress-testing architectural reliability to ensure critical citizen-facing services meet Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) targets.                                                                                             |
| <b>Pre-Migration/Post-Go-Live Review</b> | Ensuring new digital services are built on a secure, scalable foundation before launch or after major architectural changes.                                                                                                                                     |
| <b>AI Experimentation Guardrails</b>     | Identifies the prerequisites for deploying advanced data and AI services, such as Databricks and Amazon Bedrock. The assessment ensures the organisation has the necessary data governance and "sandboxed" environments to experiment safely with Generative AI. |

## 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.

| Technical Features                         | Benefits                                                                                                                                 |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Six-Pillar Well-Architected Review</b>  | <b>Holistic Governance.</b> Provides a 360-degree evaluation of workload health to identify critical architectural trade-offs.           |
| <b>FinOps &amp; Cost Optimisation</b>      | <b>Fiscal Accountability.</b> Identifies wasted spend and right-sizing opportunities to maximise taxpayer value and budget transparency. |
| <b>GreenOps &amp; Sustainability Audit</b> | <b>Net Zero Alignment.</b> Measures and reduces the carbon footprint of cloud workloads through expertise in cloud energy-efficiency.    |
| <b>Secure-by-Design Benchmarking</b>       | <b>Support for Accreditation.</b> Leverages documentation to map architecture to NCSC Cloud Security Principles.                         |
| <b>Prioritised Remediation Backlog</b>     | <b>Actionable Roadmap.</b> Delivers a delivery-ready backlog suitable for public sector governance and agile sprint planning.            |
| <b>MSP Insights</b>                        | <b>Risk Mitigation.</b> Benefits from Colibri Digital's experience as an AWS MSP Launch Partner to avoid common operational pitfalls.    |

### 3. Technical Requirements

Implementation follows the GDS Service Standard. Our assessment strictly adheres to the Technology Code of Practice, mandating a Cloud First approach and ensuring all recommended target architectures use Infrastructure as Code (IaC) for repeatability and auditability.

SC-cleared staff can be provided, subject to availability and buyer requirements, using a hybrid model of remote and on-site support.

|                                            |                                                                                                                                                                              |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Discovery</b>                           | We establish a clear understanding of the customer's technical environment and workloads, as well as high-priority pillars for review.                                       |
|                                            | Activities include the analysis of existing architecture, identification of technical debt, and review of data classification for OFFICIAL-SENSITIVE workloads.              |
|                                            | Outputs from Discovery define the success criteria and select the specific AWS accounts to be assessed.                                                                      |
| <b>Alpha<br/>(Assessment Workshops)</b>    | We conduct deep-dive workshops across the identified high-priority pillars.                                                                                                  |
|                                            | Using our internally developed Secure-by-Design documentation, we validate the configuration of tooling and security patterns against the NCSC 14 Cloud Security Principles. |
|                                            | Initial FinOps and GreenOps analysis is performed to identify immediate opportunities for cost recovery and carbon reduction.                                                |
| <b>Beta<br/>(Findings Validation)</b>      | A draft remediation backlog is produced, categorising architectural "pain points" into a prioritised roadmap.                                                                |
| <b>Live<br/>(Reporting &amp; Handover)</b> | The final production of the Well-Architected Review report and Security Assurance Pack is completed.                                                                         |
|                                            | We provide a formal handover to steady-state service management, ensuring your internal teams have the technical documentation required for operational independence.        |

## 4. Security & Quality Assurance

As an AWS Premier Partner with the Government Consulting Competency, Colibri Digital ensures all assessments meet the highest security standards.

|                      |                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personnel</b>     | SC-cleared staff can be provided, subject to availability and buyer requirements.                                                                       |
| <b>Data Handling</b> | All assessment data is stored securely in the appropriate AWS region and handled in strict accordance with GDPR and Data Protection Act 2018 standards. |
| <b>Standards</b>     | Our delivery processes are certified to ISO 27001 and Cyber Essentials Plus.                                                                            |

## 5. Support & Service Levels

This service definition covers time-bound professional services. Ongoing managed operations and 24/7 support are out of scope, unless agreed otherwise.

## 6. Constraints

The following constraints apply to the AWS Cloud Migration Readiness Assessment to ensure transparency and prevent disputes:

|                                    |                                                                                                                                            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Professional Services Scope</b> | This is a Lot 3 Cloud Support offering; it does not include the provision of cloud resources or the migration of workloads themselves.     |
| <b>Data Access</b>                 | The accuracy of the assessment is dependent on the buyer providing timely access to the platform, key personnel, and inventory data.       |
| <b>Third-Party Tooling</b>         | Use of automated discovery tools may require temporary installation within the buyer's environment, subject to internal security approval. |

## 7. Data Restoration & Disaster Recovery

Colibri Digital incorporates Resilience by Design principles into the initial discovery and architectural planning phases. This approach identifies disaster recovery (DR) requirements as a fundamental component of the proposed migration roadmap and target architectural vision.

### Our Approach to DR Planning

During the assessment, we evaluate the buyer's existing recovery requirements to inform how the proposed AWS architecture can support organisational resilience goals.

|                                       |                                                                                                                                                                                                                                                         |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Business Continuity Assessment</b> | We identify "Mission Critical" versus "Business Important" workloads to suggest a tiered DR strategy. This supports the development of cost-effective protection and sustainability targets.                                                            |
| <b>Architectural Resilience</b>       | Our architectural blueprints identify strategies—such as AWS multi-Availability Zone (Multi-AZ) and multi-region patterns—designed to mitigate the risk of single points of failure.                                                                    |
| <b>Data Protection Framework</b>      | We define recommended frameworks for automated backups using services such as AWS Backup. This includes evaluating the requirements for cross-account and cross-region replication to support recovery planning against ransomware or regional outages. |

## DR Strategy Mapping

As part of the comprehensive options appraisal, we map workloads to potential AWS DR strategies based on the buyer's stated Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO):

|                                 |                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Backup &amp; Restore</b>     | Assessment of low-cost data restoration options using Amazon S3 or AWS Backup.                        |
| <b>Pilot Light</b>              | Evaluation of minimal-footprint environments for core databases requiring rapid scaling.              |
| <b>Warm Standby</b>             | Review of scaled-down, functional versions of environments for business-critical services.            |
| <b>Multi-Site Active-Active</b> | Architectural planning for real-time traffic distribution to support near-zero downtime requirements. |

## Technical Validation & Infrastructure as Code (IaC)

To support repeatable and reliable restoration, Colibri Digital recommends a Cloud-First approach using Infrastructure as Code (IaC), e.g., Terraform or AWS Cloud Development Kit (AWS CDK).

|                                  |                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Repeatability</b>             | We advise on how DR environments can be provisioned programmatically, supporting the principle that documentation and deployment remain synchronised. |
| <b>NCSC Alignment, as agreed</b> | Restoration recommendations are reviewed against NCSC Cloud Security Principles, as agreed, with a focus on service availability and data integrity.  |

## Shared Responsibility Model

Colibri Digital provides the strategic roadmap and architectural blueprints for restoration. Under the AWS Shared Responsibility Model, the operational execution of backups and the maintenance of the recovery environment remain the buyer's or their appointed Managed Service Provider (MSP)'s responsibility. Our workshops clearly define these demarcations to inform operational clarity.

## 8. Onboarding & Offboarding

### Onboarding

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

### Offboarding & Exit

Colibri Digital follows a structured exit process designed to ensure the buyer retains full ownership of the assessment outputs and can proceed with migration planning without ongoing supplier dependency.

|                              |                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Engagement Conclusion</b> | A formal closing session to present the final Migration Readiness Report and Executive Summary.                                                         |
| <b>Access Revocation</b>     | Systematic removal of Colibri Digital's access to any buyer inventory tools or data environments provided for the assessment.                           |
| <b>Asset Transfer</b>        | Confirmation that all contracted deliverables, including the Cloud Readiness Scorecard and TCO Report, have been successfully transferred to the buyer. |

### Data Portability

All assessment artefacts are handed over in open, non-proprietary formats (e.g., PDF, CSV, or DOCX). This ensures the buyer can easily integrate findings into internal business cases or share them with other service providers for the implementation phase.

### Knowledge Handover

Knowledge transfer is integral to our Cloud Support methodology. We ensure that the buyer's internal teams are equipped to interpret and act upon the assessment findings.

|                              |                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Technical Briefing</b>    | A structured walkthrough of the Gap Analysis and Security Assurance Pack to ensure technical leads understand the rationale behind the recommendations. |
| <b>Operational Alignment</b> | Briefings for business stakeholders on the TCO model and CAF perspectives to support internal budgetary and business case justifications.               |
| <b>Skills Roadmap Review</b> | Guidance on the identified skills gaps to help the buyer plan internal training or recruitment to manage the future AWS environment independently.      |