Colibri Digital

G-Cloud 15 Service Definition

AWS Secure Multi-Account

Landing Zone

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 Multi-Account Landing Zone service provides technical support and configuration assistance to establish a scalable cloud foundation. Built with native services like AWS Control Tower, the service assists in the creation of a well-governed baseline environment perfectly suited for long-term operational use.

Designed for UK public sector organisations, the service aligns with 'secure-by-design' principles for workloads up to OFFICIAL-SENSITIVE. We provide the technical expertise to embed security controls and governance during the setup phase, supporting long-term operational use and internal assurance mandates.

Security and compliance are foundational to the landing zone architecture. The service implements robust controls aligned with the NCSC 14 Cloud Security Principles, offering a structured framework for risk management, access control, and assurance across all cloud-native applications and data platforms.

From the outset, the environment is configured to uphold UK data sovereignty, maintain a clear separation of identities and accounts, and provide comprehensive audit logging. This enables customers to retain full visibility, accountability, and control over their AI models, data assets, and application resources while strictly adhering to public sector governance and assurance mandates.

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.

We deploy a comprehensive multi-account architecture that segregates workloads into logical units (e.g., Production, Sandbox, Security, and Tooling). This environment incorporates:

Centralised Networking	Hub-and-spoke connectivity via AWS Transit Gateway with managed egress/ingress via cloud-native firewalls.
Identity & Access Management (IAM)	Integration with existing enterprise identity providers (SAML 2.0/Active Directory) using AWS IAM Identity Center for Role-Based Access Control (RBAC).
Immutable Logging	Centralised, encrypted storage of CloudTrail and Config logs in a dedicated Security account to prevent tampering.
Automated Guardrails	Preventive and detective controls (Service Control Policies and Config Rules) to enforce compliance and prevent "configuration drift."

Following deployment, we modernise all platform components using Infrastructure as Code (IaC) (Terraform or AWS Cloud Development Kit (CDK)), providing a fully

version-controlled repository. This ensures the environment is repeatable, auditable, and easily recoverable in a Disaster Recovery (DR) scenario.

Core Public Sector use cases would include:

Secure AI Experimentation & Guardrails	Provides a "Sandboxed" environment for testing Generative Artificial Intelligence (AI) and Machine Learning (ML) models. This incorporates specific AI guardrails - such as PII (Personally Identifiable Information) redaction and automated content filtering - allowing data scientists to innovate rapidly while ensuring AI outputs remain compliant with NCSC safety standards.
Centralised Data Sovereignty & Analytics	Enables the creation of a "Data Mesh" or "Data Lake" architecture where departments can securely share and analyse datasets. By leveraging native AWS services or third-party solutions within the landing zone, organisations can enforce granular access controls and ensure sensitive public sector data remains within UK residency boundaries while being accessible for cross-departmental insights.
Legacy Data Centre Migration	Provides a secure "landing point" for migrating monolithic applications while modernising the underlying network and security layers.
Digital Transformation Support	Enables rapid, self-service provisioning for DevOps teams building modern applications through "vetted" account templates that satisfy internal Information Assurance (IA) requirements.
NCSC Compliance Baseline	A pre-configured foundation for organisations required to evidence compliance with the NCSC Cloud Security Principles or Cyber Essentials Plus.
Secure Data Sharing	Facilitates inter-departmental data exchange via VPC Peering or PrivateLink within a governed, multi-account structure.

2. Features & Benefits

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

Technical Features	Benefits
Automated Account Provisioning via AWS Control Tower Account Factory.	**Accelerated Setup.** Supports the rapid creation of accounts with consistent governance baselines.
Centralised Identity & Access Management (AWS IAM Identity Center) with Entra ID/Azure AD integration.	**Access Management:** Supports SSO integration to simplify user access while maintaining RBAC.

Immutable Centralised Logging & Auditing using AWS CloudTrail and AWS Config in a dedicated account.	**Continuous Compliance & Assurance.** Provides a tamper-proof audit trail for security investigations and regulatory compliance reporting.
Automated Governance Guardrails (Service Control Policies) and hard-coded AWS region residency.	**Sovereignty Alignment:** Configured to restrict resource usage to the appropriate AWS region to support residency requirements.
Centralised Network Hub-and-Spoke architecture using AWS Transit Gateway or Cloud WAN.	**Secure Connectivity**. Simplifies inter-VPC communication and provides a scalable, secure bridge to on-premises legacy systems.
Security Tooling Integration (Security Hub, GuardDuty, and Inspector) for proactive threat detection.	**Threat Visibility:** Provides real-time visibility into vulnerabilities to assist in risk mitigation.
IaC-Driven Modernisation using Terraform or AWS CDK with version-controlled runbooks.	**Operational Excellence.** Enables repeatable, error-free deployments and simplifies "Day 2" operations like patching and backups.
Direct Mapping to NCSC Cloud Security Principles (Principles 1–14).	**Accreditation Support:** Provides mapping to NCSC principles to facilitate the buyer's internal assurance process.
Centralised Billing & Automated Resource Tagging.	**Cost Transparency.** Enables granular cloud financial management (FinOps), allowing departments to track and justify IT spend accurately.

3. Technical Requirements & Implementation

The Government Digital Service (GDS) Service Standard consists of 14 points designed to help public sector teams create and operate high-quality digital services. While often associated with user experience, it includes specific technical requirements for how services are built, hosted, and maintained.

In the context of the AWS Secure Multi-Account Landing Zone, implementation follows these standards through a structured lifecycle and specific technical mandates.

The standard is broadly categorised into three themes: understanding user needs, providing a good service, and using the right technology. Key technical points include:

Point 9	**Create a secure service that protects users' privacy**. Establishing security risks and managing them throughout the delivery lifecycle.
Point 11	**Choose the right tools and technology**. Selecting sustainable, cost-effective technology that allows for future flexibility.

Point 12	**Make new source code open**. Ensuring that code is available for others to reuse where appropriate.
Point 13	**Use and contribute to open standards and common components**. Ensuring systems can integrate easily and avoid supplier lock-in.
Point 14	**Operate a reliable service**. Minimising downtime and having a robust plan for incident response and disaster recovery.

Technical requirements are further governed by the Technology Code of Practice, which is used during GDS spend-control assessments. It mandates:

Cloud First	Consider public cloud solutions before other options.
Infrastructure as Code (IaC)	Using tools like Terraform or AWS CDK to ensure environments are repeatable and auditable.
Centralised Logging	Using tools like AWS CloudTrail and Config to provide a tamper-proof audit trail for security.

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 supporting services to be 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** — Analysis of the existing architecture to inform the recommended technical approach. 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 the proposed solution 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** Support for a pilot migration of non-critical services, identifying refinements for operational runbooks. During Beta, the service supports pilot validation of landing zone controls and operational readiness; workload migration is out of scope unless separately contracted 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 Support for production migration, including knowledge handover and stabilisation assistance. The production phase delivers the full production migration, transitioning agreed services into the target cloud environment. 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

Our Landing Zone recommendations are mapped against NCSC guidelines to provide an evidence base for the buyer's Senior Information Risk Owner (SIRO). This supports the buyer in their internal risk management and assurance activities.

NCSC Principle	Landing Zone Implementation & Evidence
1. Data in Transit Protection	Forced use of **TLS 1.2+** for all API calls; encrypted **VPC Peering** and **Transit Gateway** traffic by default.
2. Asset Protection & Resilience	Deployment across multiple **Availability Zones (AZs)**; automated EBS and RDS backups via **AWS Backup**.
3. Separation Between Users	**Multi-account architecture** ensures absolute resource isolation; VPCs provide network-level segmentation.
4. Governance Framework	Use of **AWS Control Tower** to establish a consistent, well-governed baseline environment suitable for long-term use.
5. Operational Security	**AWS Config** monitors for non-compliant changes; **Amazon GuardDuty** provides continuous threat detection.
6. Personnel Security	The service is delivered by **SC-cleared consultants**, subject to availability and buyer requirements.
7. Secure Development	Platform components are modernised using **Infrastructure as Code (IaC)** with version-controlled repositories.
8. Supply Chain Security	Adherence to G-Cloud 15 mandates, holding valid **ISO 27001** and **Cyber Essentials certifications** – see below.
9. Secure User Management	Identity federation via **IAM Identity Center**; "Joiners, Movers, Leavers" process integrated with your IdP.
10. Identity & Authentication	**MFA (Multi-Factor Authentication)** is enforced for all users; temporary credentials are used for all programmatic access.
13. Audit Information for Users	**Immutable CloudTrail logs** stored in a dedicated 'Log Archive' account with cross-account access restricted.

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. Data Restoration & Disaster Recovery

The use of Infrastructure as Code (IaC) reduces the risk of configuration drift. In a recovery scenario, the environment can be re-provisioned from version-controlled repositories to a known-good state. Our blueprints identify strategies such as Multi-AZ deployment to support service continuity during local hardware failures.

7. Constraints

The following constraints apply to the AWS Secure Multi-Account Landing Zone 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.
Maintenance Windows	While the Landing Zone is designed for high availability, certain configuration changes or platform updates may require scheduled maintenance windows, which will be agreed upon in advance to minimise disruption.
Customisation Limits	To maintain the integrity of the NCSC-aligned security posture and check that the environment remains supportable, certain core "guardrail" policies (Service Control Policies) cannot be disabled without a formal risk acceptance from the buyer.
Legacy Integration	While the service supports connectivity to on-premises systems, the speed and performance of these integrations are constrained by the buyer's existing network infrastructure and bandwidth.
Cloud Provider Availability	The service is built natively on AWS; therefore, service availability is subject to the underlying AWS Service Level Agreements (SLAs) for the appropriate AWS region.
Identity Provider Compatibility	Full automation of user management is dependent on the buyer's internal Identity Provider (e.g., Entra ID) supporting standard protocols such as SAML 2.0
Data Recovery & Restoration	The customer is responsible for managing the restoration of data and initiating disaster recovery protocols for all customer-managed applications and datasets.

8. Onboarding & Offboarding

Onboarding

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

Offboarding & Exit

We provide a structured exit process to prevent supplier lock-in. As the Landing Zone is built using native AWS services and open-standard IaC (Terraform/CDK), the buyer retains full ownership of the environment configuration.

Data Portability

All documentation, code (Git repositories), and architectural diagrams are handed over in open formats (pdf).

Knowledge Handover

We provide a structured shadowing phase where Colibri Digital acts in an observational and advisory role, ensuring the buyer's staff are confident in managing the environment independently before our access is revoked.