Colibri Digital

G-Cloud 15 Service Definition

AWS Cloud Native Identity & Access Management (IAM)

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

Identity & Access Management services incorporating AWS Cloud Native identity products provided by Colibri Digital offers UK Public Sector organisations a high-performance, enterprise-grade Identity and Access Management (IAM) solution. Our services are designed for complex, large-scale environments where "sovereignty, scalability, and security" are paramount.

As an expert implementation partner, Colibri Digital transitions organisations from fragmented legacy systems to modern, future facing solutions. We specialise in public cloud deployment however all support customers that choose to self host within their own on premise infrastructure, ensuring that identity remains a seamless bridge between our clients and their internal workforces or their end users.

Colibri Digital provides Consultancy, Architecture and Design Services as well as full platform development of IAM Platforms and Services

Technical Product Description

Common Key technical components of the delivery include:

Workforce Identity: AWS IAM Identity Center	Formerly known as AWS Single Sign-On (SSO), this is the recommended starting point for managing human users.
Customer Identity: Amazon Cognito	If you are building a web or mobile app for the public, you use Cognito rather than IAM. Contains a managed user directory that handles sign-up, sign-in, and profile management. It supports social logins (Google, Facebook, Apple) and enterprise logins via SAML/OIDC.
Workload Identity: AWS IAM (Identity & Access Management)	A high-performance, LDAPv3-compliant directory server that stores user profiles, credentials, and preferences. This is the foundational engine of AWS. While it can hold "IAM Users," in a cloud-native world, it is primarily used for Roles. Instead of using long-lived passwords or API keys, services (like an EC2 instance or a Lambda function) "assume" a role to get temporary, 1-hour credentials. IAM Roles Anywhere: A newer component that allows your on-premises servers or local containers to use IAM roles by trusting a local Certificate Authority (CA), eliminating the need for hardcoded secrets. These tools provide the "logic" and "guardrails" for your identity strategy: AWS Organizations & Service Control

Policy & Governance Components	Policies (SCPs): These sit at the top level. An SCP can say "No one in the entire company is allowed to delete audit logs," which overrules even an Admin's permissions. Amazon Verified Permissions: A specialized service for fine-grained authorization within your own custom applications (e.g., "Can User A see Document B?"). It uses a policy language called Cedar. IAM Access Analyzer: An AI-driven tool that scans your policies to find "over-privileged" users or resources that are accidentally shared with the public internet.
Zero Trust Connectivity: AWS Verified Access	A key part of modern identity is removing the need for a VPN.It grants access to internal corporate applications based on who the user is (from Identity Center) and how secure their laptop is (using signals from CrowdStrike or Jamf), rather than just whether they are on the network.

Core Public Sector Use Cases

Core Public Sector use cases would include:

Departmental "Dynamic Trust Hubs"	Colibri Digital delivers modernised IAM architectures that can unify the citizen experience across web, mobile, and IoT channels. By replacing siloed legacy IAM systems with cloud based IAM platforms, we enable organisations to deliver frictionless user journeys while leveraging automated security to drastically reduce the risk of identity fraud
NHS & Health Sector	Colibri Digital delivers modernised, clinical-grade Identity and Access Management (IAM) solutions that bridge the gap between fragmented NHS Trust boundaries. By replacing legacy "siloed" authentication with a Federated Identity Architecture, we ensure that healthcare professionals can access vital patient records securely and instantaneously, regardless of their location or the underlying legacy system
Cross Agency Identity Federation	Colibri Digital can design and deliver Federated Identity Fabrics that enable secure, seamless "Workforce Mobility" across UK Government departments. By leveraging modern protocols and cloud-native architecture, we allow public sector employees to access shared resources, cross-agency applications, and collaborative tools using their "home" department credentials. This eliminates the need for duplicate accounts, reduces the IT burden of onboarding, and strengthens the overall security posture of the public sector estate.
Legacy IAM Modernisation	Colibri Digital specialises in the systematic decommissioning of aging, on-premise identity infrastructure (such as legacy Active Directory, LDAP, or custom-built auth databases). We transition organisations to modern, cloud-native identity platforms (such as Okta, Auth0) using "low-friction" migration patterns. This ensures that as you modernise your applications, your identity layer becomes a secure, scalable enabler rather than a technical debt anchor.

2. Features & Benefits

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

Features

- **No-Code Orchestration:** Rapidly deploy user journeys using a visual interface for MFA, risk evaluation, and registration.
- **Unified Directory:** A single source of truth for workforce, customers, and "Things" (IoT), supporting multi-schema data models.
- **Hybrid Deployment Flexibility:** Support for pure SaaS, private cloud, or on-premises nodes to meet specific data residency requirements.
- **Risk-Based Adaptive Auth:** Real-time signals (IP, device, behaviour) to step up authentication only when a threat is detected.
- **Granular Authorisation:** Fine-grained access control down to the API attribute level.

Benefits

- **Reduced User Friction:** Simplifies the "Sign-in" experience for government services, increasing digital adoption.
- **Future-Proofed Compliance:** Built-in support for GDPR, Open Banking/Open Data standards.
- **Operational Cost Savings:** Modernising legacy IAM reduces the "technical debt" and maintenance costs of aging infrastructure.
- **Enhanced Resilience:** High-availability architecture ensures that essential public services remain accessible 24/7.

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 as well as their future requirements. Activities typically include:

    - Analysis of the existing architecture, platforms, user journeys 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**

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**

During Beta, the service supports a pilot migration of non-critical services, typically with limited live traffic.

Activities include:

- Migration of agreed pilot identities
- 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 prior to full-scale deployment.

4. **Live**

The production phase delivers the full production delivery, transitioning agreed services into the target 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

Colibri Digital ensures that all Ping/ForgeRock deployments meet the highest security standards:

- **ISO 27001 & Cyber Essentials Plus:** Our delivery teams operate under strictly audited internal security frameworks.
- **Zero Trust Alignment:** Every access request is verified based on identity, device posture, and network context.

5. Support & Service Levels

Not available for this offering. Ongoing 24/7 managed operations are not included but can be provided through a separate aligned managed services offering.

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.
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.
Managed Services Exclusion	This service definition covers the initial assessment, design, and modernisation; ongoing 24/7 managed operations are not included but can be provided through a separate aligned managed services offering.
Maintenance Windows	Certain modernisation activities or platform updates may require scheduled maintenance windows, which will be agreed upon in advance to minimise disruption.

7. Onboarding & Offboarding

Onboarding

Buyers are onboarded via a formal kick-off meeting typically within five working working days of a Call-Off Contract. We provide a tailored Project Initiation Document (PID) and access to our secure Jira/Confluence collaboration portal.

Offboarding & Exit

ForgeRock/Ping Identity supports Open Standards. All user data can be exported in standard LDAP/JSON formats, ensuring that the organisation can migrate to another provider if necessary without data loss.

Data Portability

ForgeRock/Ping Identity supports Open Standards. All user data can be exported in standard LDAP/JSON formats, ensuring that the organisation can migrate to another provider if necessary without data loss.

Knowledge Handover

Colibri Digital provides a structured "Shadowing" period where your internal IT staff work alongside our engineers. This is supplemented by:

- **Platform-specific Runbooks.**
- **Video-recorded Training Sessions.**
- **Code-level documentation for all orchestration flows.**