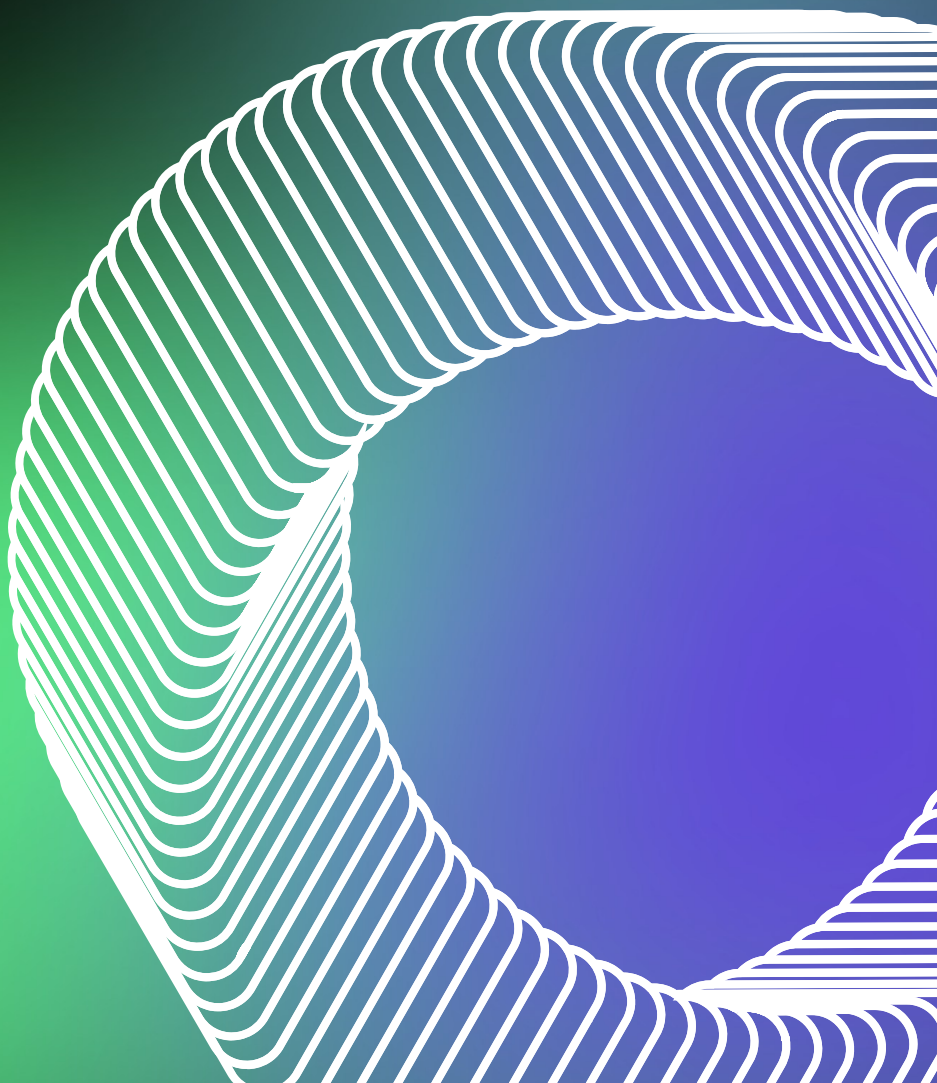
CRANMORE

SERVICE DEFINITION DOCUMENT

Cloud Landing Zone Design & Build (Azure & AWS)



73 Church View, Holywood,
BT18 9LN – United Kingdom
+44 (0)2890 394 431
info@cranmo.re

Contents

1. Purpose of this Document 3
2. Service Description 3
2.1 Overview 3
2.2 Service Components 3
2.3 Service Benefits 4
3. Delivery Approach 5
3.1 Landing Zone Service 5
3.2 Discovery & Design 5
3.3 Infrastructure-as-Code Development 5
3.4 Landing Zone Build 5
3.5 Handover & Enablement 5
4. Service Constraints 6
5. Ongoing Support 6
5.1 Support Services 6
5.2 Support Response Levels 6
6. Security and Compliance 6
6.1 Security Accreditations 6
6.2 Landing Zone Security 7
7. Pricing 7
8. Contact Information 7

1. Purpose of this Document

This document provides comprehensive information about Cranmore Consulting's Cloud Landing Zone Design & Build Services for Azure and AWS, and defines how these services are delivered to UK public sector organisations.

This Service Definition is required as part of Cranmore's listing on the G-Cloud 15 framework and conforms to the requirements specified in the Crown Commercial Service's guidance on service definition documents.

These services are designed for central government departments, local authorities, NHS organisations, and other public bodies requiring foundational cloud environments ready for secure workload deployment. Landing zones establish well-architected, governed, and secure cloud tenancies enabling organisations to deploy applications and services rapidly whilst maintaining security, compliance, and operational excellence.

2. Service Description

2.1 Overview

Cranmore delivers comprehensive cloud landing zone design and build services creating foundational cloud environments on Microsoft Azure and Amazon Web Services (AWS). Landing zones establish secure, governed, and scalable cloud tenancies with security baselines, network architecture, identity and access management, logging and monitoring, governance policies, and automation frameworks. Our services enable organisations to deploy workloads confidently knowing foundational controls, standards, and best practices are embedded from day one.

Landing zone design addresses account structure, network topology, security controls, identity architecture, operational baselines, and governance frameworks aligned with cloud provider best practices and organisational requirements. Build phase implements landing zones using Infrastructure-as-Code ensuring repeatable, auditable, and version-controlled deployments. Landing zones incorporate security by design principles including zero-trust network architecture, defence-in-depth controls, encryption, audit logging, and compliance frameworks supporting UK GDPR, Government security classifications, and public sector requirements.

Azure landing zones follow Microsoft Cloud Adoption Framework and Azure Well-Architected Framework establishing management groups, subscriptions, policies, networking, and identity foundations. AWS landing zones follow AWS Well-Architected Framework establishing organisational units, accounts, control tower, networking, and IAM foundations. Multi-account or multi-subscription architecture enables workload isolation, cost management, and governance. ISO 27001 and Cyber Essentials Plus certifications ensure security embedded throughout landing zone design and build.

2.2 Service Components

Cloud Landing Zone Design & Build Services include:

- **Design: Strategy** – Landing zone strategy defining approach, architecture patterns, and governance frameworks
- **Design: Account Structure** – Account architecture design defining Azure subscriptions or AWS accounts structure for workload isolation

- **Design: Networking** – Network architecture design establishing hub-spoke topology, connectivity, and segmentation
- **Design: IAM** – Identity and access management architecture defining authentication, authorization, and RBAC
- **Design: Security Controls** – Security baseline definition establishing foundational security controls and encryption standards
- **Design: Governance** – Governance framework establishing policies, standards, and compliance requirements
- **Design: Observability** – Logging and monitoring architecture defining audit trails, observability, and alerting
- **Build: Infrastructure as Code (IaC) Deployment** – Infrastructure-as-Code implementation using Terraform, Azure Bicep, or AWS CloudFormation
- **Build: Azure Implementation** – Azure landing zone build implementing management groups, subscriptions, policies, and networking
- **Build: AWS Implementation** – AWS landing zone build implementing organisations, accounts, control tower, and networking
- **Build: Security Implementation** – Security hardening implementing encryption, network controls, and threat protection
- **Build: Automation** – CI/CD pipeline configuration enabling automated infrastructure deployment and updates
- **Build: Documentation** – Documentation creation providing architecture diagrams, runbooks, and operational procedures
- **Build: Training** – Knowledge transfer training operations teams on landing zone management

2.3 Service Benefits

Organisations engaging Cranmore for landing zone services realise substantial advantages:

- **Accelerated Deployment** – Rapid cloud adoption with foundational environment ready for secure workload deployment
- **Security Embedded** – Security controls embedded at the foundation, aligned to NCSC cloud security principles, reducing the risk of security debt.
- **Governed Environment** – Governance foundations establishing policies and standards ensuring consistent cloud usage
- **Cloud Best Practices** – Best practice architecture following Azure and AWS well-architected frameworks
- **Infrastructure as Code (IaC) Benefits** – Infrastructure-as-Code enabling repeatable, auditable, and version-controlled infrastructure
- **Compliance Foundation** – Compliance readiness supporting UK GDPR and Government security classification requirements
- **Data residency support** – Configurations supporting UK data residency requirements where required, subject to cloud provider capabilities and Buyer configuration choices.
- **Cost Control** and **Transparency**– Cost management architecture enabling visibility and control over cloud expenditure aligned to FinOps principles
- **Scalability** – Scalable cloud foundation supporting growth from initial workloads to organisation-wide adoption
- **Operations Ready** – Operational excellence establishing logging, monitoring, and operational baselines
- **Workload Isolation** – Multi-account isolation preventing blast radius from single workload compromises

- **Reduced Toil** – Automation reducing manual effort and human error in infrastructure management
- **Sector Knowledge** – Delivery informed by public sector cloud experience, including awareness of government policy, assurance, and security expectations.
-

3. Delivery Approach

3.1 Landing Zone Service

Landing zone engagement duration depends on complexity and customisation requirements, encompassing a range of activities:

3.2 Discovery & Design

Discovery establishes requirements and designs landing zone architecture:

- Requirements workshops understanding workload types, security requirements, and compliance needs
- Current state assessment evaluating existing cloud footprint and migration requirements
- Account architecture design defining Azure subscriptions or AWS accounts structure
- Network architecture design establishing hub-spoke topology, connectivity, and segmentation
- Identity architecture design defining authentication, authorisation, and access controls
- Security baseline definition establishing encryption, logging, and control requirements
- Governance framework design defining policies, standards, and compliance controls
- Architecture documentation creating comprehensive diagrams and decision records

3.3 Infrastructure-as-Code Development

Development creates Infrastructure-as-Code for landing zone:

- IaC framework selection choosing appropriate environment
- Module development creating reusable infrastructure modules and templates
- Landing zone code development implementing account structure, networking, and security
- CI/CD pipeline configuration enabling automated testing and deployment
- Policy-as-Code implementation defining governance controls programmatically
- Code review and validation ensuring quality, security, and best practices

3.4 Landing Zone Build

Build deploys landing zone to cloud environment:

- Non-production deployment establishing test environment validating configuration
- Security hardening implementing encryption, network controls, and threat protection
- Logging and monitoring configuration establishing audit trails and alerting
- Governance policy deployment implementing organisational policies and standards
- Production deployment executing controlled rollout to production environment
- Validation testing confirming landing zone meets requirements and operates correctly

3.5 Handover & Enablement

Handover transfers landing zone to operations teams:

- Documentation handover providing architecture diagrams, runbooks, and procedures
- Knowledge transfer training operations teams on landing zone management

- Operational runbooks creating procedures for common management tasks
- Support transition establishing ongoing support arrangements
- Continuous improvement identifying opportunities for landing zone enhancement

4. Service Constraints

To support successful landing zone outcomes:

- **Account and Environment access:**
- Availability of appropriate access to cloud accounts, subscriptions, and organisational context supports effective landing zone design and configuration.
- **Coordination:** Cranmore works collaboratively with the Buyer to coordinate design workshops, architecture reviews, and technical decision-making.
- **Workload and Compliance Requirements:** Landing zone effectiveness is enhanced where workload requirements, security controls, and compliance needs are defined and shared by the Buyer.
- **SME availability:** Access to cloud, security, networking, and platform subject matter experts supports robust design and validation.
- **Engagement:** Regular buyer participation in design reviews and testing supports delivery
- **Operations readiness:** Successful handover is supported by Buyer operational team readiness, including agreed support models, monitoring, and operating procedures

5. Ongoing Support

5.1 Support Services

Cranmore provides comprehensive landing zone support:

- **Expert Leadership** – Cloud Architect providing technical leadership and cloud platform expertise
- **Progress Reporting** – Regular progress updates through design reviews and demonstrations
- **Collaboration** – Collaborative tools access via Confluence, Miro, Git repositories
- **Email Support** – Email support for queries (info@cranmoreconsulting.com)
- **Phone Support** – Telephone support during business hours (028 9042 1238)

5.2 Support Response Levels

Incident response based on business impact:

- **Priority 1 (Major Impact):** 15 minutes response, 6 hours resolution target
- **Priority 2 (High Impact):** 1 hour response, 8 hours (one working day) resolution target
- **Priority 3 (Moderate Impact):** 4 hours response, 3 working days resolution target
- **Priority 4 (Minor Impact):** 1 day response, 10 working days resolution target

6. Security and Compliance

6.1 Security Accreditations

Cranmore maintains:

- **ISO 27001** – International standard for information security management
- **Cyber Essentials Plus** – Independently verified cyber security controls

- **Security Clearance (SC)** – Key personnel hold UK Security Check clearance enabling work with OFFICIAL and OFFICIAL-SENSITIVE data

6.2 Landing Zone Security

All landing zones implement security by design including zero-trust network architecture, defence-in-depth controls, encryption at rest and in transit, comprehensive audit logging, identity and access management, threat protection, security monitoring, and UK GDPR compliance. Landing zones align with Azure and AWS security best practices and public sector requirements.

7. Pricing

Landing zone services priced based on complexity and customisation:

- **Design & Build:** Typically delivered on a fixed-price basis, agreed in advance based on the landing zone architecture and requirements
- **Optional Enhancements:** Time and Materials pricing may be used for agreed enhancements or extensions, priced separately
- **Payment Terms:** Invoiced monthly in arrears; 30-day payment terms

All pricing excludes VAT.

Cloud provider infrastructure costs (Azure/AWS) are separate and paid directly to cloud providers.

See pricing documents for more information.

8. Contact Information

Primary Contact

Fergus McGrath
Sales Director
Cranmore Consulting
Mobile: 07912 777717
Email: fergus@cranmoreconsulting.com

Service Desk

Telephone: 028 9042 1238
Email: info@cranmoreconsulting.com

Registered Office

Cranmore Consulting Ltd
73 Church View, Holywood
BT18 9LN
United Kingdom

G-Cloud 14 Listing

https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/479964968691217