



marino_

G-Cloud 15

Lot 3: Cloud Support / Cloud Migration Planning Service Definition

Document control

Framework	G-Cloud 15 (RM1557.15)
Service name	Cloud Support
Lot	Lot 3
Service category	Cloud Migration Planning (Marino Modernise)
Supplier name	Marino Software Limited
Version	1.0
Date	27th January 2026
Service owner	Ed Melvin
Public contact email	info@marinosoftware.com

Table of Contents

1. Purpose of this document	4
2. Service summary.....	4
2.1. What the service is	4
2.2. Who the service is for.....	4
2.3. Key features	4
2.4. Key benefits	5
3. Scope of service	6
3.1. In scope	6
3.2. Out of scope.....	6
4. Delivery approach	7
4.1. Delivery model	7
4.2. Roles and responsibilities	7
5. Onboarding and mobilisation	8
5.1. Buyer prerequisites.....	8
5.2 Mobilisation activities	8
6. Support and service management	8
6.1. Support hours.....	8
6.2. Incident management.....	8
7. Security and assurance	9
8. Data protection	9
9. Performance and reporting	10
10. Exit and portability	10
11. Pricing overview.....	10
12. Marino Software.....	10
12.1. About Marino Software	10
12.2. Contact Details	11

1. Purpose of this document

This Service Definition describes how Marino Software delivers Cloud Support Services under G-Cloud 15 Lot 3 (Cloud Support: Cloud Migration Planning).

It is intended to help public sector buyers understand:

- what the service includes and excludes
- the features and benefits of the service
- how it is delivered
- buyer and supplier responsibilities
- how the service is priced and supported

This document should be read alongside:

- the G-Cloud 15 Pricing Document
- the supplier's Service Levels
- the CCS G-Cloud 15 Call-Off Contract

2. Service summary

2.1. What the service is

Marino Modernise helps organisations transform legacy applications into secure, scalable, cloud-native platforms. Through structured discovery, modern architecture, data and security by design, and AWS-native delivery, Marino enables incremental or full modernisation with strong observability, lifecycle support, and knowledge transfer.

2.2. Who the service is for

- Central government departments
- Arm's length bodies and agencies
- Local authorities
- Health, education and emergency services
- Public sector organisations at any stage of cloud adoption

2.3. Key features

- Application modernisation strategy and delivery for legacy and cloud systems
- Discovery and assessment of existing applications, risks, and technical debt

- System design and assurance for scalable, maintainable cloud-native architectures
- Incremental or full re-architecture to reduce risk and improve time-to-value
- AWS cloud integration using managed services and established best practices
- Infrastructure as code for repeatable, secure, multi-environment deployments
- Data architecture modernisation including storage, streaming, and real-time processing
- Security by design including identity management, encryption, and network controls
- Observability, monitoring, and alerting to support operational readiness
- Ongoing support, enhancements, and knowledge transfer throughout application lifecycle

2.4. Key benefits

- Reduces technical debt and improves long-term application maintainability
- Accelerates delivery through incremental modernisation and automated pipelines
- Improves system scalability and performance using cloud-native architectures
- Reduces operational risk through observability, monitoring, and proactive alerting
- Improves security posture through identity management, encryption, and network controls
- Enables faster recovery and resilience through automated, repeatable environments
- Improves data access and insights through real-time data pipelines
- Reduces deployment errors using infrastructure as code and CI/CD
- Supports informed decision-making through structured discovery and assessment
- Builds internal capability through collaboration and knowledge transfer

3. Scope of service

3.1. In scope

The service may include any combination of the following, depending on buyer needs:

- Application and infrastructure discovery
- Cloud readiness assessments
- Migration strategy and roadmap (modernisation-focused)
- Risk, dependency and complexity analysis
- Cost modelling and optimisation planning
- Cloud set-up and configuration
- Reviews against the AWS Well Architected Program
- Network, identity and access configuration
- Security baseline configuration
- Monitoring and logging set-up
- Re-hosting, re-platforming or re-factoring support
- Validation and post-migration assurance
- Knowledge transfer and documentation

3.2. Out of scope

Unless explicitly agreed in writing, the following are excluded:

- End-user device support, including desktops, laptops, and mobile devices
- Application redevelopment beyond the agreed modernisation or migration scope
- Business process redesign or organisational change management activities
- Procurement or management of buyer-owned third-party software or contracts
- Software licence, subscription, and usage costs from third-party providers
- Ongoing managed service operations unless explicitly included in the service
- On-site delivery or support, unless agreed in advance as an optional service
- Data ownership, data quality remediation, or content cleansing activities
- Responsibility for legacy system decommissioning unless explicitly agreed

4. Delivery approach

4.1. Delivery model

Services are delivered primarily remotely, using secure collaboration tools. Onsite delivery can be provided where agreed.

Delivery follows an iterative, risk-managed approach aligned to government cloud best practice.

- **Discovery and assessment** - Assess applications, architecture, technical debt, risks, and constraints.
- **Modernisation strategy and roadmap** - Define target architecture and prioritised, incremental modernisation approach.
- **Design and preparation** - Design cloud-native architecture, security, data, and operational foundations.
- **Modernisation delivery** - Re-host, re-platform, or refactor applications within agreed scope.
- **Testing and validation** - Validate functionality, performance, security, and operational readiness.
- **Handover and assurance** - Provide documentation, knowledge transfer, and post-modernisation assurance.

4.2. Roles and responsibilities

Area	Supplier	Buyer
Modernisation discovery and planning	✓	Support
Target architecture and design	✓	Approve
Cloud environment configuration	✓	Approve
Security architecture and baseline configuration	✓	Approve
Application modernisation delivery	✓	Support
Access provisioning and user management	Support	✓
Data ownership and data governance		✓

Testing and acceptance	Support	✓
Service governance and delivery oversight	✓	✓

5. Onboarding and mobilisation

5.1. Buyer prerequisites

- Named service owner and technical contact
- Timely access to environments and documentation
- Agreement on scope and priorities
- Access to required cloud platforms

5.2 Mobilisation activities

- **Kick-off meeting** – Establishes shared understanding of objectives, roles, and delivery approach.
- **Confirmation of scope and success criteria** – Agrees services, deliverables, assumptions, and measurable outcomes.
- **Access and security onboarding** – Sets up required system access in line with security requirements.
- **Delivery plan and schedule** – Defines milestones, dependencies, and agreed delivery timelines.

6. Support and service management

6.1. Support hours

Standard: Monday–Friday, UK business hours

Extended / 24x7: Available as a service option

6.2. Incident management

Incidents are logged, prioritised and managed using ITIL-aligned processes.

Severity	Description
Sev 1	Critical service outage
Sev 2	Major service degradation

Sev 3	Minor issue or workaround available
Sev 4	Service request or query

Target response and resolution times are defined in the Service Levels document.

7. Security and assurance

The service is delivered in line with recognised security best practice to protect buyer systems and data.

Access is restricted to authorised personnel using least-privilege principles, with clear separation of responsibilities and secure configuration baselines in place. Access and controls are reviewed regularly.

Where applicable, the supplier maintains recognised security certifications, including ISO/IEC 27001 and Cyber Essentials or Cyber Essentials Plus.

The service is supported by documented business continuity arrangements, regular verification of backups, and support for buyer disaster recovery testing to ensure service resilience.

8. Data protection

The service handles personal data in accordance with buyer instructions and applicable data protection requirements. Personal data is processed only for the purposes agreed with the buyer and is stored and processed in agreed geographic locations.

Any sub-processors used to support service delivery are disclosed to the buyer and managed in line with contractual and data protection obligations.

Data is retained only for the duration of the contract and is securely deleted on service exit or termination, in accordance with agreed retention and disposal procedures.

9. Performance and reporting

Service performance and delivery are supported through clear and regular reporting. Buyers receive periodic service reports covering delivery progress, incident and change activity, and key operational insights.

Where applicable, capacity and cost information is provided to support informed decision-making.

Continuous improvement recommendations are shared to help buyers optimise outcomes and plan next steps.

10. Exit and portability

10.1 Exit support

The supplier supports an orderly exit, including:

- Knowledge transfer
- Documentation handover
- Data export in agreed formats

10.2 Exit fees

Any exit charges are clearly stated in the Pricing Document. If none apply, this will be explicitly confirmed.

11. Pricing overview

Pricing is transparent and based on:

- Time-boxed discovery and modernisation assessment engagements
- Day or sprint-based rates for design and modernisation delivery
- Scope defined by agreed modernisation approach (re-host, re-platform, refactor)
- Incremental delivery phases to control cost and reduce risk
- Optional on-site support priced separately, by prior agreement

Full details are provided in the G-Cloud 15 Pricing Document.

12. Marino Software

12.1. About Marino Software

Marino Software delivers secure, scalable mobile, cloud and AI-powered solutions that help organisations innovate and grow. We combine expert

consultancy, intuitive design and robust engineering to transform digital experiences and modernise systems, whether building apps, migrating to the cloud or optimising platforms. Trusted partners to global brands, we solve complex challenges with clarity and precision, driving measurable value for our clients.

12.2. Contact Details

Area	Name	Email
Service enquiries	Ed Melvin	ed.melvin@marinosoftware.com
Support	Client-specific addresses are provided for each organisation.	
Security	n/a	security@marinosoftware.com
Data Protection	Cara Ludlow	cara.ludlow@marinosoftware.com