

Service Definition: Cloud IT Support Services

1. Service Overview

Dule Dynamix Ltd will provide Cloud IT Support Services to buyers within the G-Cloud 15 framework with expert assistance to plan, deploy, manage, secure, and optimise cloud environments. The service covers Microsoft Azure, Microsoft 365, AWS, Google Cloud, and hybrid infrastructures. It includes proactive monitoring, incident resolution, service requests, optimisation, governance, and strategic guidance.

The service is designed to help organisations reduce operational overhead, improve resilience, enhance security, and ensure compliance with UK government standards.

2. Key Features & Capabilities

2.1 Service Desk & End-User Support

- Multi-channel support (portal, email, phone, chat)
- Tiered support (T1–T3)
- Incident management and service request fulfilment
- Knowledge-base access and self-service options

2.2 Cloud Platform Management

- Azure, AWS, Google Cloud, alternative and Microsoft 365 administration
- Identity and access management
- Configuration, patching, and policy enforcement
- Backup, disaster recovery, and business continuity

2.3 Monitoring & Automation

- 24/7 monitoring of cloud workloads
- Automated alerting and remediation
- Performance tuning and cost optimisation
- Capacity planning and forecasting

2.4 Security & Compliance

- Threat detection and response
- Vulnerability management
- Logging, auditing, and SIEM integration
- Compliance alignment with:
 - Cyber Essentials / Plus
 - ISO 27001
 - NCSC Cloud Security Principles

- WCAG 2.2 A (where applicable)

2.5 Consultancy & Advisory

- Cloud strategy and roadmap development
- Architecture design and review
- Migration planning and execution
- Governance frameworks and FinOps guidance

3. Service Scope

The service covers:

Included

- Cloud platform support (Azure, AWS, GCP, M365)
- Incident management
- Service requests
- Monitoring and alerting
- Security operations
- Backup and DR management
- Cost optimisation
- Monthly reporting and service reviews

Optional Add-Ons

- On-site support
- Advanced security operations (SOC/SIEM)
- Cloud migration projects
- Application modernisation

4. Service Levels (SLAs)

Service Component	SLA
Service Desk Availability	24 hours
Incident Response (T1)	1 hour
Incident Response (T2)	1 hour
Incident Response (T3)	1 hour
Service Request Response	1 business day
Monthly Reporting	Delivered within 5 working days of month end

Custom SLAs available for critical environments.

5. Onboarding & Transition

5.1 Onboarding Activities

- Kick-off meeting and requirements review
- Access and permissions setup
- Tooling integration (monitoring, ticketing, logging)
- Knowledge transfer and documentation review
- Baseline health assessment

5.2 Transition from Existing Supplier

- Handover of documentation and credentials
- Review of existing configurations
- Risk assessment and mitigation planning
- Parallel support period (if required)

Typical onboarding time: **2–6 weeks**, depending on complexity.

6. Offboarding & Exit Management

A structured exit process ensures continuity and avoids vendor lock-in.

Exit Deliverables

- Full documentation handover
- Transfer of credentials and configurations
- Export of monitoring and ticketing data
- Knowledge transfer sessions
- Optional support during transition to new supplier

Exit support is charged at standard day rates.

7. Pricing Model

Pricing is transparent and published in accordance with G-Cloud rules.

Pricing Options

- **Per-user per-month** (for end-user support)
- **Per-environment per-month** (for cloud platform support)
- **Time & materials** (for consultancy and project work)
- **Fixed-price packages** (optional)

No hidden fees. No minimum contract term beyond G-Cloud call-off requirements.

8. Technical Requirements

To deliver the service, the customer must provide:

- Administrative access to relevant cloud platforms
- Network connectivity for monitoring agents (if required)

- Named contacts for approvals and escalations
- Existing documentation (where available)

9. Data Security & Protection

The service adheres to UK government security expectations.

Security Controls

- ISO 27001-aligned processes
- UK-based support teams
- Data stored and processed in UK regions
- MFA enforced for administrative access
- Encryption in transit and at rest

Data Protection

- GDPR-compliant
- No customer data stored outside approved systems
- Data retention policies aligned with customer requirements

10. Accessibility

All customer-facing portals and documentation are designed to meet **WCAG 2.2 A**, with selected AAA criteria implemented where feasible.

11. Service Management

Customers receive:

- Dedicated service manager
- Monthly service reviews
- Quarterly roadmap and optimisation sessions
- Access to service performance dashboards

12. Dependencies

- Customer cloud subscriptions and licensing
- Customer responsibility for application-level support unless otherwise agreed
- Third-party vendor support contracts (if applicable)

13. Customer Responsibilities

- Provide timely access and approvals
- Maintain accurate asset and user information
- Ensure compliance with organisational policies
- Report incidents promptly

14. Benefits to Public-Sector Buyers

- Predictable costs
- Reduced operational burden
- Improved security posture
- Faster issue resolution
- Access to certified cloud specialists
- Alignment with government digital and cloud strategies

15. Governing Law

This Agreement is governed by and construed in accordance with the laws of England and the parties submit to the exclusive jurisdiction of the English courts.