

Service Definition Document: Sterling Cloud Support Services (Lot 3)

1. What the Service Is

This service delivers comprehensive managed cloud support for private, public, and hybrid environments, including IaaS, PaaS/SaaS, and application management. Our highly motivated, secure, and knowledgeable team provides proactive monitoring, incident resolution, security hardening, architecture design, workload migration, performance optimisation, cost management, vendor selection, staff training, and ongoing advisory services. It supports UK public sector organisations in maintaining reliable, compliant, and efficient cloud operations across selected vendors, including AWS, Azure, Google Cloud, Oracle, VMware, and others, in line with NCSC principles and government standards.

2. Levels of Data Backup, Restore, and Disaster Recovery

As a support service, we assist buyers in implementing and managing data backup, restore, and disaster recovery processes tailored to their cloud environments. This includes guidance on configuring automated backups (e.g., snapshots, replication), defining RTO/RPO objectives, and conducting regular DR testing. For managed private/hybrid setups, we provide business continuity planning, failover strategies, and support for offline media in disconnected environments. Restore support ensures quick recovery via self-service tools or assisted interventions, with full audit trails.

3. Onboarding and Offboarding Support

Onboarding involves detailed discovery sessions, environment assessments, and customised support plans. We offer documentation, online training modules, workshops, and knowledge transfer to empower buyer teams. Assisted migration and setup are included, with a dedicated TAM for initial guidance. Offboarding includes the handover of configurations, documentation, and support history to ensure a smooth transition. Data access and extraction from supported clouds are facilitated, with no retention of buyer data after the contract.

4. Service Constraints

Support is primarily remote via secure channels; onsite visits are available at extra cost. Standard hours are 09:00–17:30 UK business days (excluding holidays); 24/7 requires premium tiers. Customisation is flexible but depends on the buyer-provided access and environment details. In fully disconnected setups, offline methods apply for updates and reporting. Response times/effectiveness rely on timely buyer cooperation. All constraints are outlined in the call-off agreement.

5. Service Levels

We commit to response SLAs: 4 hours initial (standard), 1 hour (priority/enterprise), with resolution targets based on severity. Availability of support channels is 99.9% during covered hours. Performance metrics include proactive issue detection and optimisation



recommendations. 24/7 coverage is optional for critical needs. SLAs exclude buyer-induced delays or force majeure, with credits for breaches.

6. After Sales Support

Support includes email, ticketing, web chat, and MFA-protected portal access. Tiers range from standard (business hours) to enterprise (24/7 proactive). Dedicated TAM and Cloud Support Engineers provide strategic advice, reviews, and escalations in higher tiers. Our team ensures secure, knowledgeable assistance for troubleshooting, optimisation, and compliance.

7. Any Technical Requirements

Buyers need secure remote access (e.g., VPN or bastion hosts) and valid cloud credentials. Compatible with major platforms; minimum requirements include modern browsers for portals and standard APIs for integration. For disconnected environments, offline tools and media are used. Staff should have basic cloud familiarity; training provided.

8. Outage and Maintenance Management

Outages in supported environments are proactively monitored; incidents are reported via the dashboard, email alerts, and the API. We follow predefined playbooks for common events, with root cause analysis post-resolution. Maintenance coordination minimises impact, with advance notice and buyer involvement.

9. Hosting Options and Locations

As a support service, we manage buyer-hosted environments (private on-premises/UK data centres, public/hybrid clouds). Support ensures UK data residency compliance. Multi-site resilience is advised and supported.

10. Access to Data (Upon Exit)

Buyers retain data control. We assist with extraction using cloud-native tools or offline methods, and provide handover reports. No data is stored by us post-contract.

11. Security

Security processes follow ISO 27001 and NCSC guidelines, with zero-trust access, MFA, RBAC, and encrypted communications. Vulnerability assessments, incident response (1-4 hours), and change management ensure secure support. Full details on our website.