

Service Definition: Cloud Support Services

1. Overview – What the Service Is

Our Cloud Support Services provides structured, ongoing technical and operational support for cloud-based platforms, infrastructure, and applications. The service is designed to ensure that cloud environments remain reliable, secure, performant, and aligned with business needs throughout their lifecycle. It supports organisations before, during, and after cloud adoption by providing expert assistance across incident management, monitoring, optimisation, and continuous improvement.

The service is suitable for organisations operating public cloud, private cloud, or hybrid cloud environments and can be tailored to support infrastructure, platforms, applications, or a combination of all three. Cloud Support Services are delivered by experienced cloud engineers and support specialists who work closely with customer teams to maintain service stability, reduce operational risk, and improve long-term value from cloud investments.

2. Scope of the Service

Cloud Support Services typically include:

- Proactive monitoring of cloud services and workloads
- Incident management and fault resolution
- Configuration and operational support
- Performance and cost optimisation recommendations
- Support for platform updates and patches
- Advisory support for platform improvements and changes
- Regular service reporting and review meetings

The service can operate as a fully managed support model or as a co-managed arrangement alongside internal IT teams.

3. Data Backup, Restore, and Disaster Recovery

As part of Cloud Support Services, we support the design, operation, and validation of backup, restore, and disaster recovery arrangements. This includes ensuring that appropriate backup mechanisms are in place for data, applications, and configurations, aligned with the customer's business criticality and regulatory obligations.

Backups are monitored for successful completion, and restore processes are periodically validated to ensure recoverability. Where required, we support the implementation and testing of business continuity and disaster recovery plans, including failover procedures and recovery exercises.

Recovery objectives, such as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), are agreed with the customer during onboarding and reviewed periodically to ensure they remain appropriate as services evolve.

4. Onboarding and Offboarding Support

Onboarding

Onboarding to Cloud Support Services follows a structured process to ensure a smooth transition into support. This includes:

- Review of the existing cloud environment and architecture
- Confirmation of scope, responsibilities, and escalation paths
- Secure access setup using least-privilege principles
- Baseline health checks and risk identification
- Documentation review and knowledge transfer

This process ensures that the support team has sufficient understanding of the environment to provide effective and timely assistance.

Offboarding

Offboarding is handled in a controlled and secure manner. This includes:

- Revocation of access and credentials
-

- Support for data extraction or handover to another provider
- Transfer of operational documentation and service records
- Confirmation of secure deletion where required

The offboarding process ensures continuity for the customer while protecting data and security.

5. Service Constraints

Cloud Support Services are typically delivered remotely. On-site support can be provided by agreement where required.

Maintenance activities, configuration changes, and platform updates are carried out within agreed maintenance windows to minimise disruption. Emergency changes are handled through defined incident management processes.

The level of customisation supported depends on the underlying cloud platform and agreed scope. Highly bespoke or non-standard configurations may require additional assessment or commercial agreement.

6. Service Levels and Availability

Service levels are defined through agreed Service Level Agreements (SLAs). These typically include:

- Incident response times based on severity
- Target resolution or workaround times
- Support hours, such as business hours or 24/7 coverage
- Escalation procedures and governance

Availability and performance metrics are monitored using cloud-native and third-party tools. Regular reporting provides transparency on service health, incidents, and trends.

7. After-Sales and Ongoing Support

After initial onboarding, Cloud Support Services operate as an ongoing engagement focused on stability and improvement. This includes:

- Continuous monitoring and alerting
- Incident analysis and root cause investigation
- Proactive recommendations for improvement
- Periodic service reviews and reporting
- Support for audits, compliance checks, and operational reviews

The service is designed not only to react to issues but also to reduce the likelihood of future incidents through proactive management.

8. Technical Requirements

To deliver Cloud Support Services effectively, the following are typically required:

- Secure access to cloud subscriptions or accounts
- Access to monitoring, logging, and alerting tools
- Integration with service management or ticketing systems
- Visibility into architecture documentation and change history

All access is controlled, logged, and reviewed regularly.

9. Outage and Maintenance Management

Incidents and outages are managed using a structured incident management framework. This includes:

- Detection and triage
 - Communication with stakeholders
 - Resolution and service restoration
 - Post-incident review and reporting
-

Planned maintenance activities are communicated in advance, with clear impact assessments and rollback plans where appropriate.

10. Hosting Options and Locations

Cloud Support Services support environments hosted across:

- Public cloud platforms
- Private cloud environments
- Hybrid cloud architectures

Support can be provided across approved geographic regions to meet data residency and regulatory requirements.

11. Access to Data Upon Exit

Customer data remains the property of the customer at all times. Upon exit, we support:

- Data export in agreed formats
- Verification of data completeness
- Secure deletion of retained data in line with contractual and regulatory requirements

No customer data is retained beyond agreed retention periods.

12. Security and Data Protection

Security is integral to the delivery of Cloud Support Services. The service follows established security best practices, including:

- Least-privilege access controls
 - Strong authentication and identity management
 - Encryption of data in transit and at rest
-



- Audit logging and activity monitoring
- Compliance with applicable data protection regulations

All support activities are carried out in a manner that protects the confidentiality, integrity, and availability of customer systems and information.

