

Service Definition: Set Up and Migration Services

1. Overview – What the Service Is

Set Up and Migration Services provide the practical implementation required to establish cloud environments and migrate existing workloads from legacy platforms into cloud-based software and hosting services. The service covers the end-to-end process of preparing target environments, consolidating workloads, transferring data, and validating that services operate correctly after migration.

This service is designed to minimise disruption to business operations while ensuring that migrated systems are secure, reliable, and aligned with agreed architecture and governance standards. It supports a wide range of workload types, including email systems, file stores, calendars, applications, user permissions, metadata, and interdependent components.

2. Scope of the Service

Set Up and Migration Services typically include:

- Preparation and configuration of target cloud environments
 - Identity and access configuration
 - Network connectivity and security setup
 - Migration of workloads such as:
 - Emails and mailboxes
 - Files and document repositories
 - Calendars and collaboration data
 - Applications and services
 - User accounts and permissions
 - Document types and related metadata
-

- Linked components and compound structures
- Data validation and integrity checks
- Decommissioning or handover of legacy systems

The service supports both lift-and-shift migrations and modernisation approaches where appropriate.

3. Data Backup, Restore, and Disaster Recovery

Before any migration activity begins, existing backup arrangements are reviewed and validated to ensure data can be recovered if required. Where necessary, additional pre-migration backups are taken to provide a secure rollback point.

During migration, data is transferred using secure, controlled processes with verification checks to confirm completeness and accuracy. Post-migration, backup and recovery mechanisms are implemented or updated in the target environment to align with business continuity requirements.

Disaster recovery considerations are built into the target design, including geographic redundancy, failover strategies, and recovery testing where applicable.

4. Onboarding and Offboarding Support

Onboarding

Onboarding to Set Up and Migration Services begins with a detailed readiness assessment. This includes confirming scope, success criteria, dependencies, and migration sequencing. Technical access is established securely, and migration plans are finalised in collaboration with stakeholders.

The onboarding phase ensures that all parties understand timelines, responsibilities, communication channels, and risk mitigation strategies before migration activities commence.

Offboarding

Offboarding includes formal acceptance of migrated services, confirmation of data integrity, and documentation handover. Where agreed, legacy systems are decommissioned in a controlled manner, ensuring that data retention and compliance obligations are met.

Access to source systems is removed, and any temporary migration tooling is retired securely.

5. Service Constraints

Migration activities are subject to agreed maintenance windows and change management processes to minimise business disruption. Some legacy systems may have technical limitations that restrict migration approaches or require remediation before migration.

Highly bespoke applications or unsupported platforms may require additional analysis or custom migration tooling.

The service is typically delivered remotely, with on-site support available by agreement.

6. Service Levels and Delivery Management

Service levels for Set Up and Migration Services are defined around delivery milestones rather than operational SLAs. These include:

- Migration readiness sign-off
- Successful completion of migration waves
- Validation and acceptance criteria
- Hypercare and stabilisation periods

Clear communication is maintained throughout delivery, with progress updates, issue tracking, and escalation procedures.

7. After-Sales and Post-Migration Support

Following migration, a defined hypercare period provides enhanced support to address any issues that arise as users transition to the new environment. This includes troubleshooting, configuration adjustments, and performance tuning.

After hypercare, support can transition into ongoing cloud support services, ensuring continuity and long-term stability.

8. Technical Requirements

Effective delivery of Set Up and Migration Services typically requires:

- Administrative or delegated access to source and target systems
- Network connectivity between environments
- Access to identity and directory services
- Availability of subject matter experts for validation and testing

All access is granted on a least-privilege basis and reviewed regularly.

9. Outage and Maintenance Management

Migrations are planned to minimise downtime, using phased approaches, parallel running, or off-hours cutovers where appropriate. Detailed rollback plans are defined to address unexpected issues.

Planned outages are communicated in advance, with clear timelines and impact assessments. Emergency issues are handled through established incident management processes.

10. Hosting Options and Locations

Set Up and Migration Services support:

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

Target hosting locations are selected based on data residency, compliance, performance, and resilience requirements.

11. Access to Data Upon Exit

Customer data remains fully owned by the customer throughout the migration process. Upon completion or exit, all migrated data is accessible in the target environment, and any residual data held by migration tooling is securely deleted.

Documentation and migration artefacts are provided to support future operations.

12. Security and Data Protection

Security is embedded throughout Set Up and Migration Services. This includes:

- Encryption of data in transit
- Secure handling of credentials and secrets
- Audit logging of migration activities
- Validation of access controls post-migration

All activities are conducted in line with data protection regulations and organisational security policies to protect the confidentiality, integrity, and availability of customer systems and information.

