Service Definition: Cloud Migration Planning Services

1. Overview – What the Service Is

Cloud Migration Planning Services provide structured, expert-led planning and advisory support to help organisations prepare for the transition from legacy or on-premise systems to cloud-based software and hosting services. The service focuses on understanding the current environment, defining the target cloud architecture, identifying risks and dependencies, and producing a clear, actionable migration roadmap.

This service is designed for organisations at an early stage of cloud adoption or those seeking to modernise existing environments in a controlled and cost-effective manner. It ensures that migration decisions are informed by technical, operational, financial, and security considerations, reducing uncertainty and avoiding disruption during later implementation phases.

---

2. Scope of the Service

Cloud Migration Planning Services typically include:

- Discovery and assessment of existing systems and workloads
- Application and data dependency mapping
- Cloud readiness and suitability assessments
- Target architecture and landing zone design
- Migration strategy definition, including sequencing and prioritisation
- Risk identification and mitigation planning
- Cost modelling and forecasting
- Creation of a detailed migration roadmap and delivery plan

The service is vendor-neutral and can support public cloud, private cloud, or hybrid cloud strategies.

---

3. Data Backup, Restore, and Disaster Recovery Considerations

As part of the planning process, existing backup, restore, and disaster recovery arrangements are reviewed and documented. This includes assessing current recovery capabilities, identifying gaps, and defining how backup and disaster recovery requirements will be met or improved in the target cloud environment.

The service ensures that business continuity requirements are understood early and embedded into the target design. Recommendations may include changes to backup frequency, retention, geographic redundancy, or recovery testing processes.

While no changes are made to live systems during planning, the outputs clearly define how recovery objectives such as RTO and RPO will be achieved post-migration.

---

4. Onboarding and Offboarding Support

Onboarding

Onboarding begins with stakeholder engagement and discovery workshops to understand business objectives, constraints, and success criteria. This is followed by structured technical discovery activities, including documentation review, interviews with system owners, and analysis of usage patterns.

Access requirements are kept minimal and are typically read-only to reduce risk. All data gathered during onboarding is handled securely and used solely for planning purposes.

Offboarding

At the conclusion of the service, all deliverables are formally handed over. This includes architecture designs, assessment reports, cost models, and migration plans. Any access provided during onboarding is removed, and collected data is returned or securely destroyed as agreed.

---

5. Service Constraints

Cloud Migration Planning Services are advisory and planning-focused. They do not include hands-on migration or configuration changes unless explicitly combined with setup and migration services.

The accuracy of planning outputs depends on the quality and completeness of information provided. Where legacy systems lack documentation or visibility, assumptions and risks are clearly documented.

The service is typically delivered remotely, although in-person workshops can be arranged if required.

---

6. Service Levels and Delivery Management

Service delivery is governed by agreed milestones and timelines rather than operational SLAs. A delivery plan is agreed at the outset, outlining key phases, dependencies, and review points.

Regular progress updates are provided, and findings are validated with stakeholders to ensure alignment and accuracy. Any changes to scope or assumptions are managed through a controlled change process.

---

7. After-Sales and Ongoing Support

Following completion of the planning phase, after-sales support includes clarification sessions, roadmap walkthroughs, and support for internal approval processes. The service also provides continuity into subsequent phases, such as setup, migration, or ongoing support, if required.

This ensures that planning outputs remain relevant and actionable rather than theoretical.

---

8. Technical Requirements

To deliver effective migration planning, the following inputs are typically required:

- High-level architecture diagrams and system inventories
- Access to usage and performance data where available
- Information on licensing, contracts, and compliance requirements
- Input from technical and business stakeholders

Where direct system access is not possible, structured interviews and documentation reviews are used.

---

9. Outage and Maintenance Considerations

No production changes are made as part of Cloud Migration Planning Services. As a result, there is no impact on system availability or maintenance schedules.

However, the service includes analysis of how future migrations can be executed with minimal downtime. This includes recommendations for migration windows, phased cutovers, and rollback strategies.

---

10. Hosting Options and Locations

Migration planning supports a range of hosting models, including:

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

Hosting region selection considers data residency, regulatory requirements, latency, and resilience needs. Recommendations are aligned with organisational policies and applicable regulations.

---

11. Access to Data Upon Exit

All assessment data, findings, and planning outputs are owned by the customer. Upon exit, deliverables are provided in agreed formats, and any customer data held by the service provider is returned or securely deleted.

No customer data is retained beyond the agreed engagement period.

---

12. Security and Data Protection

Security and data protection are central to Cloud Migration Planning Services. All information collected is handled in line with data protection legislation and organisational security policies.

Access to customer information is limited to authorised personnel and is logged and reviewed. Planning outputs include security considerations such as identity management, network segmentation, encryption, and monitoring, ensuring that security is built into the target design from the outset.