Cloud Data Migration Checklist

This checklist is designed for:
Project managers, cloud architects and IT leaders overseeing cloud data migrations, from planning through to cutover.

Cloud data migration isn't as simple as "moving data to the cloud." It's a specialised discipline with its own risks, constraints and failure modes.

Cloud data migration focuses on transferring databases, file systems and bulk data into platforms such as AWS and Microsoft Azure. Each platform has its own tools, limits and architectural assumptions that directly affect how data can be ingested and managed. This is fundamentally different from lifting and shifting servers or rebuilding applications. Why? Because cloud platforms impose strict requirements on how data is ingested and managed. Get it wrong, and data loss or corruption can quickly turn into a costly, business-impacting event.

Interactive brings hands-on experience across AWS, Azure and Interactive's own Private Cloud, helping teams migrate data to cloud platforms while maintaining compliance and operational continuity. To help guide your successful cloud data migration, we've put together this comprehensive checklist.

The checklist specifically focuses on data, not VMs or infrastructure. Think on-prem databases to cloud-native databases, file servers to object storage, or hybrid cloud environments where data needs to move safely and gradually, without disrupting operations.

We cover the three core migration types: database migration, file and storage migration and large-scale bulk transfers.

Designed for Australian organisations, it factors in data sovereignty, Australian cloud regions and the reality of bandwidth limits.

For broader planning, see Interactive's cloud migration services, the Data Migration Framework, or the wider migration checklist library.

What Makes Cloud Data Migration Different

Cloud data migration introduces challenges that don't exist in traditional environments. These include:

Australian data residency:

Regulated data must stay within Australian cloud regions throughout the migration.

Bandwidth constraints:

Large data volumes require careful network planning, particularly where legacy infrastructure is involved.

Transfer costs:

Cloud providers charge for data ingress and egress.

Tools:

Each platform brings its own cloud-native tools, including AWS DataSync and Azure Data Box, alongside hybrid connectivity options like Direct Connect and ExpressRoute.

Storage tier selection:

Requires finding the right balance between performance, cost and accessibility.

Your Complete Cloud Data Migration Checklist

This checklist is designed to help you facilitate a smooth, zero-downtime cloud data migration - while maintaining compliance and optimising costs. Following this process will help you avoid the common mistakes that can derail poorly planned migrations.

Assessment and Planning

Successful cloud data migration starts with a clear understanding of what data's moving, how fast you can realistically move it and which regulatory constraints apply. This is the pre-work that must be done before you select your tools or begin the migration.

Calculate total data volumes: Measure the size of all databases, file systems and object stores. Account for data growth during the migration window.

Assess network bandwidth: Identify your available bandwidth between on-premises environments and the cloud, including contention and peak-usage constraints.

Determine data sovereignty requirements: Map obligations under relevant regulatory frameworks, such as the Australian Privacy Principles or sector-specific regulations such as APRA CPS 234.

Select Australian cloud regions: Confirm appropriate regions such as Sydney (ap-southeast-2) or Melbourne based on residency and latency needs.

Estimate transfer duration: Develop realistic transfer timelines based on data volume, bandwidth and tooling limitations.

Calculate transfer costs: Factor in data egress charges, cloud ingress and ongoing storage tier costs.

Identify data dependencies: Document applications, services and integrations that rely on the data.

Choose migration approach: Online transfer, physical devices (AWS Snowball, Azure Data Box) or hybrid models.

Plan for business continuity: Define how systems access data during the migration.

Define success criteria: Data integrity, cutover timing and post-migration performance benchmarks.

Australian environments often require coordination with NBN or telco carriers to support temporary bandwidth increases and careful Sydney vs Melbourne region selection to balance latency and compliance.

Once you've ticked off those planning and assessment requirements, you're ready to facilitate the transfer.

AWS DataSync and Data Transfer

AWS DataSync is purpose-built for large-scale cloud data migration to AWS, automating data movement while optimising network usage and validating data integrity. It's the most common cloud migration tool among Australian organisations because it addresses the real constraints of bandwidth, scale and reliability.

AWS DataSync implementation checklist:

Deploy AWS DataSync agent:

Install the agent as a VM on VMware, Hyper-V, or EC2 within the source environment.

Confirm network connectivity to source storage and outbound access to AWS endpoints before proceeding.

Configure source location:

Point the agent to the source NFS or SMB file shares, or supported self-managed object storage.

Validate permissions and run a small test scan to confirm all required data is visible.

Set up AWS destination:

Choose Amazon S3, Amazon EFS, or Amazon FSx for Windows File Server based on access patterns, performance requirements and downstream application needs.

Confirm lifecycle policies and storage class settings upfront to avoid post-migration rework.

Configure DataSync tasks:

Define transfer schedules, bandwidth limits, include/exclude rules and overwrite behaviour.

Start with conservative throttling during business hours, then increase throughput during off-peak windows.

Enable encryption:

Enable TLS encryption for data in transit and confirm AWS-managed encryption is enabled at rest on the destination service.

Validate IAM roles and access policies before the first full transfer.

Run initial test transfers:

Execute a partial migration to validate performance, permissions and task configuration.

Review logs and error handling before scaling up to full datasets.

Monitor transfer progress:

Track throughput, latency, errors and completion status using Amazon CloudWatch.

Adjust parallelism and task timing to maximise throughput without impacting production workloads.

Validate data integrity:

Use DataSync's built-in checksum validation to confirm source and destination consistency.

Spot-check critical directories or datasets before declaring the migration complete.

Optimise performance:

Remove temporary agents, tasks and infrastructure once validation is complete to avoid ongoing cost.

AWS data transfer options to consider:

AWS Direct Connect: Dedicated links (1–100 Gbps) for predictable, high-volume transfers.

AWS Snowball: Physical devices for multi-terabyte datasets where bandwidth is constrained.

AWS Transfer Family: Managed SFTP, FTPS, or FTP for ongoing synchronisation to S3.

S3 Transfer Acceleration: Faster internet-based transfers using AWS edge locations.

Australian considerations:

Use the Sydney region (ap-southeast-2) to meet data sovereignty requirements.

Plan Direct Connect via Sydney or Melbourne facilities.

Factor Snowball availability and shipping timelines into your cloud data migration strategy.

Azure Data Migration

Azure provides a mature set of cloud-native tools for cloud data migration, with particular strength in structured database workloads. For many Australian organisations, the Azure Database Migration Service (DMS) is the preferred approach for moving production databases into Azure with minimal disruption.

Azure data migration checklist:

Use Azure Database Migration Service (DMS):

Use Azure DMS to manage migrations into Azure SQL, Azure Database for MySQL, or PostgreSQL, rather than building custom tooling.

Confirm the target platform and supported migration paths before proceeding.

Run pre-migration assessments:

Use Azure DMS assessments to identify compatibility issues, deprecated features, unsupported objects and potential migration blockers.

Remediate issues upfront to avoid delays during execution.

Configure secure source connections:

Establish secure connectivity to on-premises SQL Server, Oracle, MySQL or PostgreSQL environments.

Validate credentials, firewall rules and network latency before starting migration jobs.

Create and scope migration projects:

Define source and target platforms, select offline or online migration modes and group databases logically by risk and complexity.

Start with lower-risk workloads to validate the approach.

Execute staged migrations and cutover:

Use continuous synchronisation for online migrations to keep source and target aligned.

Plan and execute final cutover during approved maintenance windows to minimise downtime.

Use Azure Data Box where bandwidth is constrained:

Deploy Azure Data Box devices (up to 100 TB per unit) for large datasets or sites with limited network capacity.

Validate data ingestion and reconciliation once data is uploaded to Azure.

Implement Azure ExpressRoute for predictable performance:

Establish dedicated private connectivity to Azure for consistent throughput, lower latency and improved reliability during migration.

Enable Azure File Sync for hybrid access:

Use Azure File Sync to maintain local file access while data is progressively migrated to Azure file services.

Monitor and adjust throughout the migration:

Track migration status, throughput and errors using Azure Monitor.

Adjust scheduling, batching and synchronisation settings to avoid production impact.

Australian considerations:

Select Australia East (Sydney) or Australia Southeast (Melbourne) regions to meet data residency requirements.

Confirm Azure's Australian government and regulated-industry certifications.

Plan ExpressRoute connectivity via Sydney, Melbourne, Perth, or Canberra as part of a robust Azure data migration strategy.

File and Storage Migration

File and storage cloud data migration requires a different approach to databases or applications. Success depends on understanding data volumes, user access patterns and how people actually work during and after the transition.

OneDrive and SharePoint migration checklist:

Assess file server data volumes: Measure total size, file counts and folder structures to identify any complexities and migration risks.

Use the OneDrive Migration Tool: Leverage Microsoft's Migration Manager for large-scale, permission-aware bulk transfers.

Configure OneDrive synchronisation: Enable staged migration. This minimises user disruptions and allows them to gradually adapt to the new environment, without complicating the migration itself.

Migrate SharePoint document libraries: Preserve permissions, metadata and version history to maintain business continuity.

Plan user cutover: Coordinate communications, training and access reconfiguration ahead of go-live.

Google Drive migration checklist:

Use Google Workspace migration tools

Use Google's native migration tools to move data from file servers, SharePoint or other cloud storage platforms into Google Drive.

Validate permissions, folder structures and ownership mapping before running large migrations.

Enable hybrid access during transition

Configure Drive for desktop (formerly Drive File Stream) to provide users with local-style file access while data is progressively migrated.

Communicate access changes clearly to minimise user disruption.

Support cross-account migrations

Migrate data between Google Workspace accounts to support organisational consolidation, divestment or cloud exit scenarios.

Confirm sharing settings, ownership transfer and retention policies post-migration.

Validate and finalise

Spot-check critical folders, confirm user access and clean up temporary migration permissions once the transition is complete.

Cloud storage best practices:

Select appropriate storage tiers: Balance frequent access requirements against archive cost savings.

Implement lifecycle policies: Automate transitions to cold storage based on access patterns.

Enable backup and versioning: Use native version controls to protect data post-migration.

Testing and Validation

Comprehensive testing and validation ensure your cloud data migration delivers accurate, secure and performant outcomes. This phase confirms that data has transferred correctly, applications function as expected and regulatory requirements continue to be met.

Testing and validation checklist:

Perform data reconciliation: Compare source and cloud record counts and checksums.

Validate data integrity: Confirm no data loss or corruption occurred during transfer.

Test application functionality: Ensure applications operate correctly with cloud-hosted data.

Measure cloud performance: Compare latency and throughput against on-premises baselines.

Verify data sovereignty compliance: Confirm data resides in approved Australian regions.

Test backup and recovery: Validate cloud backup and restore procedures.

Validate security controls: Confirm encryption, access controls and audit logging operate as intended. This step closes the loop on your cloud migration checklist and reduces risk before final cutover.

Essential Cloud Migration Tools

Cloud providers offer specialised tools to simplify cloud data migration, reduce transfer time and minimise cost. Selecting the right tools depends on data type, volume and how quickly data must be moved with minimal disruption.

AWS cloud data migration tools:

AWS DataSync: Automated data transfer with built-in bandwidth optimisation and data integrity checks.

AWS Database Migration Service: Database migrations with continuous replication to reduce downtime.

AWS Snowball and Snowcone: Physical data transport for multi-terabyte datasets where bandwidth is constrained.

AWS Transfer Family: Managed SFTP and FTPS endpoints for ongoing data ingestion to Amazon S3.

Azure cloud migration tools:

Azure Data Box: Physical data transport devices supporting transfers up to 100 TB.

Azure Database Migration Service: Managed database migrations to Azure SQL and open-source platforms.

Azure File Sync: Hybrid file server migration with staged cutovers.

AzCopy: Command-line utility for high-performance blob and file transfers.

Related Data Migration Resources

Use the below resources to support your data migration planning and execution:

- **Data Migration Framework:**
  Strategic guidance for planning and governing complex data migration programs.
- **Data Migration Checklist Library:**
  Checklists covering cloud, on-premises and hybrid migration scenarios.
- **Cloud Data Migration Checklist:**
  Detailed guidance for migrating cloud-hosted databases.
- **Cloud Migration Services:**
  End-to-end cloud strategy and migration support.

Planning a database migration?

Interactive's cloud and data migration services support Australian enterprises with certified AWS and Azure specialists. We also operate our own Interactive private cloud, designed for regulated organisations that need the flexibility and performance of cloud with the assurance of an owned environment. No matter your cloud destination, we deliver proven methodologies, data sovereignty expertise and 24/7 local support across Australia.

CONTACT US