

## CLOUD AND INFRASTRUCTURE

# Cloud readiness and migration checklist

Prepare the transfer of a working service

Prepare a service for migration by checking dependencies, target operations, data reconciliation and recovery. Define cutover conditions, cost ownership and a complete handover before retiring the original environment.

---

### THE WORK

Trace the operating service, rehearse the transfer and agree the target environment, recovery route and acceptance evidence.

### THE RESULT

A migration readiness decision and cutover record with clear responsibility for the resulting service.

#### INSIDE THIS GUIDE

02–03 Service and dependencies

05 Cost and cutover planning

08–09 Verification checks

04 Data and target operations

06–07 Recovery and acceptance

10 Cutover decision

# Define the service and objective

## Purpose and participants

A cloud migration changes more than the location of an application. It can alter identity, network paths, data movement, operating responsibilities, recovery arrangements and the cost of running the service. Readiness depends on understanding those changes before the production cutover.

This checklist supports a migration decision for a defined application or service. It brings application, infrastructure, security, data, finance and operational owners into one review. Use it to establish the migration boundary, investigate dependencies, prepare the target environment and agree the conditions for moving production work.

The resulting decision should identify what is ready, what requires action and which conditions would prevent or pause the migration. Keep the assessment connected to the actual cutover plan so the migration team can act on it during the move.

## Service boundary and decision owners

Name the business service, accountable owner and operating outcome. Identify the applications, databases, integrations and support processes within scope. Record the intended benefit in terms that can be checked after the migration, such as a required support model, a recoverability improvement, a platform constraint or a capacity requirement.

Choose the migration approach according to the service and its dependencies. Moving the current system with limited change has different testing and operating implications from replacing components or redesigning the application. Record which parts will change, which will remain and why the approach fits the objective.

Confirm the business calendar and acceptable interruption. Identify events that constrain the move, including batch processing, reporting, transaction peaks and supplier availability. Keep the planned migration window separate from the recovery objectives used if the cutover fails.

Establish the decision owners for readiness, cutover, recovery and business acceptance. Name a person responsible for maintaining the integrated plan across teams. A dependency assigned to another department still needs an agreed owner and completion condition in the migration record.

# Map the operating dependencies

## Trace connections and ownership

Trace the application in use. Include identity providers, name resolution, network routes, databases, file stores, messaging, email, payment or booking services, scheduled jobs and monitoring. Record both incoming and outgoing connections, including work that occurs outside normal office hours.

For each dependency, establish the endpoint, owner, authentication method, data exchanged and expected timing. Confirm whether the target environment changes address ranges, certificates, firewall rules, allowlists or permissions. Identify who can make those changes and how they will be verified.

## Hidden work and transition boundaries

Review dependencies that are easy to miss: a script on an administrator's device, a shared folder used by an overnight job, an external partner sending files to a fixed address, or an application using a local configuration file. Inspect logs and actual transaction paths alongside architecture diagrams.

Group components that must move or be tested together. Record interfaces that will cross the old and new environments during transition. Check latency, connectivity and operational ownership for that temporary arrangement. A technically reachable connection still needs to meet the requirements of the business transaction.

# Data and target operations

## Authority, transfer and write control

Identify the authoritative data stores and the information each contains. Record volume, change rate, retention, access requirements and dependencies on format, time zone, encoding or precision. Determine what will be copied, transformed, archived or left in place.

Choose a transfer and synchronisation method that fits the source, target and permitted interruption. Establish how changes made during migration will be captured and reconciled. Define which system can accept writes at each stage, and how duplicate or out-of-order processing will be detected.

## Identity and operating responsibility

Confirm the account or subscription structure, identity model, privileged access, network boundaries and naming arrangements. Verify that the people who will operate the service can perform their responsibilities and that access can be revoked through the normal organisational process.

Establish configuration management, logging, monitoring, backup, recovery and deployment arrangements. The migration should enter a service that can be operated consistently after the project team leaves. Assign owners for platform and application tasks, including the boundaries of any managed service.

## Reconciliation and acceptance

Prepare validation before moving production data. Row counts or file counts can detect some errors, but the team also needs checks relevant to the information and the service. Verify key records, relationships, permissions, totals where meaningful, and the ability to complete the business task against the migrated state.

Define how reconciliation differences will be investigated and who can accept the result. Preserve the evidence needed to trace a migrated record without exposing unnecessary personal or confidential information. Test the transfer, transformation and validation sequence together so the elapsed time includes the work required to establish correctness.

## Capacity, security and data controls

Check resource quotas, certificates, capacity limits and supplier dependencies before the cutover window. Test the important transaction paths from the locations and devices that need them. Verify administrative access through the approved route as well as customer-facing access.

Document the changes required for security and data handling. Confirm the approved locations for the information, the access model, encryption arrangements and any constraints identified by the responsible data or security owner. Evaluate the actual target configuration rather than assuming that moving to a managed platform establishes the necessary controls.

## 04 / REVIEW

# Cost and cutover planning

## Steady-state and transition costs

Estimate the operating costs that follow from the intended architecture and usage. Include compute, storage, backups, data transfer, managed services, support and licences where relevant. Record the quantity and pricing assumptions used so the estimate can be reviewed when demand or configuration changes.

Identify transition costs separately. Parallel operation, data transfer, engineering effort, testing, supplier support and temporary capacity can make the migration period materially different from steady-state operation. Assign an owner to ending temporary arrangements when their purpose is complete.

## Trade-offs, allocation and review

Compare the estimate with the service objective. A lower infrastructure price does not establish a lower total operating cost if support effort, connectivity or recovery requirements increase. Review the trade-off with the people who own the resulting service and budget.

Set up the allocation and review mechanism before launch. Ensure the team can connect expenditure to a service and owner, recognise an unexpected change and decide what to do about it. Record the first cost review point and the information needed to compare the actual service with the estimate.

## Runbook and rehearsal

Write an ordered runbook that covers preparation, final synchronisation, traffic or workflow switching, validation and acceptance. Give each consequential step an owner, prerequisite, expected evidence and decision point. Include communication to users, support teams and connected service owners.

Rehearse the sequence in an environment that can establish the important dependencies and timing. Record what the rehearsal actually tested and what remains dependent on the production environment. Resolve failed steps and repeat the affected sequence before treating the issue as closed.

# Recovery and readiness

## Decision points and new transactions

Define the conditions for stopping before cutover, pausing during cutover and recovering after traffic has moved. Identify who can make each decision and keep their contact route available. Establish a last decision point that leaves enough time for the chosen recovery action within the business constraint.

Check the consequences of new transactions in the target environment. Returning network traffic to the earlier system does not automatically preserve work written after cutover. Decide how that work will be reconciled, transferred or otherwise handled, and confirm the business authority for the decision.

Verify the recovery route, including credentials, connectivity, backups, configuration and the operating steps required to use the recovered service. If returning to the previous environment is no longer feasible, document the available recovery plan and its limitations before authorising the move.

## Readiness decision and acceptance

Review the service boundary, dependency map, target controls, data validation, cost ownership and rehearsed cutover together. A completed infrastructure task cannot compensate for an unresolved dependency that prevents the business service from operating.

Classify outstanding items by consequence. Identify issues that block the move, conditions that require explicit acceptance, and work that can be completed after migration without compromising the agreed service. Give each accepted condition an owner, temporary control and review point.

Record the readiness decision against the named source and target configurations. Material changes after review should reopen the affected checks. Confirm that the runbook, contact routes and decision authority are available to the team carrying out the cutover.

Use the readiness record to state what will be checked in production and who will accept the service. Avoid a blanket approval that leaves operators to interpret the decision during the migration window.

# Accept the migrated service

## Verify the business service

Validate the business task in the target environment, including relevant exception and recovery paths. Confirm that users, support staff, scheduled jobs, reports and connected systems can operate with the new state. Resolve data reconciliation differences according to the agreed acceptance process.

Maintain explicit observation ownership during the initial operating period. Include the full business cycle needed to exercise the migrated service. Monitor operational health, task outcomes, support demand and cost according to the review plan.

## Handover and transition retirement

Hand over the service with current access, configuration, operating guidance, recovery instructions and known conditions. Confirm that the receiving team accepts responsibility and can perform the required tasks. Keep unresolved migration work connected to named owners in the normal operating process.

Retire the old environment only after the authorised decision that it is no longer required for service, recovery, retention or investigation. Remove obsolete routes and access, end temporary spending and confirm that connected teams have updated their records. Preserve the information needed to understand and operate the final service.

## 07 / VERIFICATION

# Migration readiness checks

Mark a condition verified only after reviewing its evidence. Keep unresolved conditions and accepted exceptions in the decision record.

|    |                                                                                                                                                                    |                                                                                                                    |          |                          |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------|--------------------------|
| 01 | <b>Service boundary and objective</b><br><br>Confirm the intended operating outcome, included components, business constraint and accountable owners.              | <b>Evidence to retain</b><br>Named source and target service scope, objective and decision authority.              | Verified | <input type="checkbox"/> |
| 02 | <b>Application and operating dependencies</b><br><br>Exercise relevant connections, permissions, scheduled work and interfaces that cross the transition boundary. | <b>Evidence to retain</b><br>Dependency map, owning contacts and observed connection/transaction checks.           | Verified | <input type="checkbox"/> |
| 03 | <b>Data movement and reconciliation</b><br><br>Rehearse transfer and synchronisation; verify record meaning and control which environment may accept writes.       | <b>Evidence to retain</b><br>Transfer result, reconciliation criteria, difference owner and write-control plan.    | Verified | <input type="checkbox"/> |
| 04 | <b>Target controls and operations</b><br><br>Check access, security, monitoring, backup, recovery and the platform/application responsibility boundary.            | <b>Evidence to retain</b><br>Verified target configuration, restoration evidence and accepted operating ownership. | Verified | <input type="checkbox"/> |
| 05 | <b>Capacity, cost and support</b><br><br>Check quotas and transaction paths; assign costs, support responsibilities and an owner for temporary expenditure.        | <b>Evidence to retain</b><br>Capacity checks, cost assumptions, allocation and support acceptance.                 | Verified | <input type="checkbox"/> |

## 08 / VERIFICATION

# Migration readiness checks — continued

Mark a condition verified only after reviewing its evidence. Keep unresolved conditions and accepted exceptions in the decision record.

|    |                                                                                                             |                                                                                                                   |                          |
|----|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------|
| 06 | <b>Cutover and recovery rehearsal</b>                                                                       | Verified                                                                                                          | <input type="checkbox"/> |
|    | Run the ordered sequence and prove the recovery route, including target writes after traffic has moved.     | Evidence to retain<br>Timed rehearsal results, corrected failures and an agreed reconciliation/recovery decision. |                          |
| 07 | <b>Conditions and decision authority</b>                                                                    | Verified                                                                                                          | <input type="checkbox"/> |
|    | Identify what blocks the move, what is explicitly accepted and who may pause, recover or accept production. | Evidence to retain<br>Readiness decision tied to configurations, named authorities and time-bound conditions.     |                          |
| 08 | <b>Business acceptance and retirement</b>                                                                   | Verified                                                                                                          | <input type="checkbox"/> |
|    | Verify the full operating cycle and define when the original environment can be retired.                    | Evidence to retain<br>Business acceptance criteria, observation owner and retirement requirements.                |                          |

# Cutover decision record

Complete the decision against the reviewed configuration. Record unresolved conditions, the authorised owner and the evidence required for acceptance.

## Scope and readiness

Service, source environment and target environment

Migration window and business constraint

Final synchronisation and write-control approach

Validation evidence and unresolved conditions

## Authority and acceptance

Pause condition and last safe recovery decision

Cutover lead, recovery authority and acceptance owner

Decision, production acceptance and next review