

Technology Migration Readiness Checklist

Use this checklist before approving development, data transfer, or production cutover.

1. Business Goals and Scope

- The reason for migration is clearly defined.
- Expected business outcomes are measurable.
- Included applications, data, infrastructure, and integrations are listed.
- Excluded features and systems are documented.
- Budget, timeline, owners, and approval authority are confirmed.
- Migration has been compared with retaining, refactoring, rebuilding, or replacing the system.

2. System Inventory

- Applications, modules, frameworks, and versions are documented.
- Databases, servers, cloud services, and storage systems are listed.
- Unsupported or end-of-life technologies are identified.
- Third-party tools, licences, and vendors are recorded.
- Source code, deployment processes, and technical documentation are accessible.
- Business and technical owners are assigned.

3. Dependency Mapping

- APIs and third-party integrations are mapped.
- Authentication, permissions, and user roles are documented.
- Scheduled jobs, webhooks, queues, and background processes are identified.
- Shared databases, files, and services are documented.
- Environment variables, certificates, URLs, and credentials are reviewed.
- Business-critical workflows are mapped and approved.

4. Risk Assessment

- Technical, security, data, performance, and downtime risks are documented.
- Each major risk has a likelihood and impact score.
- High-risk items have mitigation plans and owners.
- Maximum acceptable downtime is defined.
- Maximum acceptable data loss is defined.
- Business-continuity requirements are approved.

5. Target-Platform Evaluation

- The target platform supports required workflows and integrations.
- Security, compliance, scalability, and availability requirements are supported.
- Team skills and training requirements are assessed.
- Vendor support and long-term maintenance are evaluated.
- Data portability and vendor lock-in risks are reviewed.
- Total migration and operating costs are estimated.
- High-risk assumptions are tested through a pilot or proof of concept.

6. Migration Strategy

- Each workload is marked for retain, retire, rehost, replatform, replace, or refactor.
- Migration phases and workload sequence are defined.
- A pilot migration is planned where required.
- Project, technical, data, security, and business owners are assigned.
- A formal change-control process is in place.
- The migration runbook is documented.

7. Data Migration

- Source data volume, quality, and growth are assessed.
- Source and target schemas are mapped.
- Transformation and cleanup rules are documented.
- Obsolete, duplicate, and invalid data is identified.
- Full and incremental transfer methods are defined.
- The source of truth is clear during each migration phase.
- A complete backup has been created and restoration tested.

8. Data Validation

- Source and target record counts will be compared.
- Required fields, duplicates, and relationships will be checked.
- Financial totals and calculated values will be reconciled.
- Historical records, permissions, and audit data will be validated.
- Automated validation scripts are prepared.
- Acceptable mismatch thresholds are approved.
- Data owners will provide final sign-off.

9. Security and Compliance

- Sensitive and regulated data is classified.
- Encryption is enabled in transit, at rest, and in backups.
- Least-privilege access is applied.
- Secrets and credentials are stored securely.
- Temporary migration access has an expiry plan.
- Security logging and alerting are enabled.
- Data residency, retention, and compliance requirements are reviewed.
- Temporary migration files have a secure deletion process.

10. Testing

- Business-critical workflows are tested.
- User roles and permissions are tested.
- APIs and third-party integrations are tested.
- Data reconciliation is complete.
- Performance and load testing are complete.
- Security testing is complete.
- User-acceptance testing is approved.
- Critical defects are resolved before cutover.

11. Cutover Planning

- The migration date and cutover window are approved.
- The change-freeze period is defined.
- Final backup and data synchronization steps are documented.
- Every cutover task has an owner and expected duration.

- Go or no-go checkpoints are defined.
- Vendors, support teams, and decision-makers are available.
- Stakeholder and customer communication is prepared.
- The cutover runbook has been rehearsed.

12. Rollback Readiness

- Rollback triggers are clearly defined.
- The source application and database can be restored.
- Traffic can be redirected to the original system.
- New transactions can be reconciled.
- DNS, configuration, integration, and deployment rollback steps are documented.
- Rollback ownership and authority are assigned.
- Rollback procedures have been tested.
- The source system will remain available during stabilization.

13. Post-Launch Monitoring

- Application uptime, errors, and response times are monitored.
- Database, infrastructure, and integration performance are monitored.
- Security alerts and backup monitoring are active.
- Transactions and business metrics are compared with the original baseline.
- Support tickets and user issues are tracked.
- Incident ownership and escalation procedures are defined.
- Cloud and software costs are monitored.
- A post-migration audit is scheduled.

14. Final Go-Live Check

- Final backup completed
- Change freeze active
- Data transfer completed
- Data validation passed
- Critical workflows passed
- Authentication and permissions passed
- Integrations passed
- Performance checks passed
- Security checks passed

- Monitoring and alerts active
- Rollback remains available
- Business owner approved go-live

Final Approval

Migration Lead: _____

Business Owner: _____

Technical Owner: _____

Data Owner: _____

Security Reviewer: _____

Go or No-Go Decision: _____

Approved Migration Date: _____