



Cloud Migration Checklist

A step-by-step guide covering discovery, landing zones, security, and cutover best practices.

1. Discovery & Assessment

Task	Description
Identify business drivers	Clarify the primary motivations for moving to the cloud – whether reducing costs, increasing agility, improving scalability, or enhancing resilience. Define success metrics tied to these goals.
Application inventory	Catalogue all existing applications, workloads, servers, and integrations. Identify interdependencies, legacy components, and third-party systems that may impact migration sequencing.
Assess cloud readiness	Evaluate workloads using a readiness framework (such as CAF, MRA, or CCA) to determine which should be rehosted, replatformed, refactored, or retired.
Performance baseline	Document current CPU, memory, I/O, and latency benchmarks for accurate cloud sizing and post-migration validation.
Cost and licensing analysis	Estimate potential costs in the cloud compared to current on-prem expenses, accounting for compute, storage, and licensing implications.
Identify compliance constraints	Review requirements such as GDPR, ISO 27001, SOC 2, or industry-specific frameworks to ensure compliance alignment from the outset.

2. Design & Planning

Task	Description
Select migration approach	Decide the best-fit migration strategy—lift and shift, replatforming, or refactoring—based on workload criticality and modernisation potential.
Define target architecture	Develop a high-level architecture including network topology, security controls, compute/storage layers, and identity management integration.

Choose cloud services	Select managed services (databases, messaging, compute) that balance cost, performance, and operational simplicity across providers.
Define migration waves	Group workloads into waves according to complexity, dependencies, and business impact to ensure controlled progression.
Plan downtime windows	Collaborate with business stakeholders to identify acceptable cutover periods that minimise disruption.
Build rollback plan	Create and test a rollback procedure to restore systems in case of migration failure.
Define KPIs and SLAs	Set quantifiable targets for uptime, response time, and recovery objectives to measure migration success.

3. Landing Zone Setup

Task	Description
Establish account or project structure	Set up a multi-account or multi-project model to isolate workloads by environment or business unit for better governance.
Configure identity and access	Integrate SSO or directory services with fine-grained role-based access control (RBAC/IAM). Enforce least privilege and MFA.
Networking design	Build secure VPC/VNet architectures with routing, peering, and connectivity to existing networks via VPN or dedicated links.
Logging & monitoring	Enable centralised monitoring and alerting using native or third-party tools for visibility across environments.
Security baselines	Apply organisation-wide security policies, service control policies, and baseline configurations aligned to CIS or NIST standards.
Backup and DR strategy	Define a robust backup and disaster recovery plan with clear recovery time and recovery point objectives (RTO/RPO).
Infrastructure as Code (IaC)	Adopt automation for consistent environment provisioning using tools such as Terraform, Pulumi, or CloudFormation.

4. Security & Compliance

Task	Description
Identity hardening	Use federated identity, enforce MFA, rotate credentials regularly, and restrict use of long-lived access keys.
Data protection	Encrypt data at rest and in transit. Implement customer-managed encryption keys where required for compliance.
Network security	Enforce segmentation with firewalls, private subnets, and restricted routing. Implement WAFs and intrusion detection as needed.
Logging & audit trails	Enable comprehensive logging for security and compliance auditing, centralising them in a secure storage location.
Vulnerability scanning	Perform regular scans pre- and post-migration to identify weaknesses and ensure patching processes are in place.
Compliance validation	Map configurations to compliance frameworks such as CIS, ISO27001, or SOC 2 and maintain evidence through automation.

5. Migration Execution

Task	Description
Pilot migration	Start with a non-critical system to validate tooling, runbooks, and cutover procedures before scaling up.
Data migration	Use appropriate services or tools for transferring databases and files while maintaining data integrity and security.
Application migration	Execute workload migration in pre-defined waves. Validate dependencies, configurations, and integrations after deployment.
Validation testing	Conduct smoke, performance, and user acceptance testing to confirm operational readiness.
Cutover plan	Coordinate final syncs, DNS changes, and user redirections to complete transition with minimal downtime.
Decommission old systems	Safely shut down and remove legacy infrastructure once validation and backups are complete.

6. Post-Cutover & Optimization

Task	Description
Validate service functionality	Ensure all applications, integrations, and endpoints are operational post-migration.
Monitor and tune	Collect and review metrics to rightsize resources, improve performance, and manage costs efficiently.
Implement cost governance	Establish budgets, alerts, and resource tagging to maintain financial control.
Conduct security review	Re-run vulnerability and compliance assessments to confirm adherence to security baselines.
Documentation & handover	Update operational runbooks, architectural diagrams, and knowledge bases for long-term maintainability.
Continuous improvement	Incorporate lessons learned into CI/CD pipelines and refine processes for future migrations.

7. Best Practice Tips

Task	Description
Automate everything	Use automation for provisioning, configuration, and validation to reduce risk and increase repeatability.
Shift security left	Integrate compliance and vulnerability scanning early in CI/CD workflows.
Tag all resources	Apply consistent tagging for ownership, cost tracking, and lifecycle management.
Use managed services	Leverage managed databases, Kubernetes, and monitoring solutions to minimise operational overhead.
Review regularly	Perform monthly reviews of performance, cost, and compliance posture to maintain optimisation.

Partner with the experts.

Jassoft specialises in delivering secure, automated, and compliant cloud foundations from discovery through to optimisation.

If you'd like help turning this checklist into a tailored migration plan, get in touch:

 contact@jassoft.co.uk |  www.jassoft.co.uk