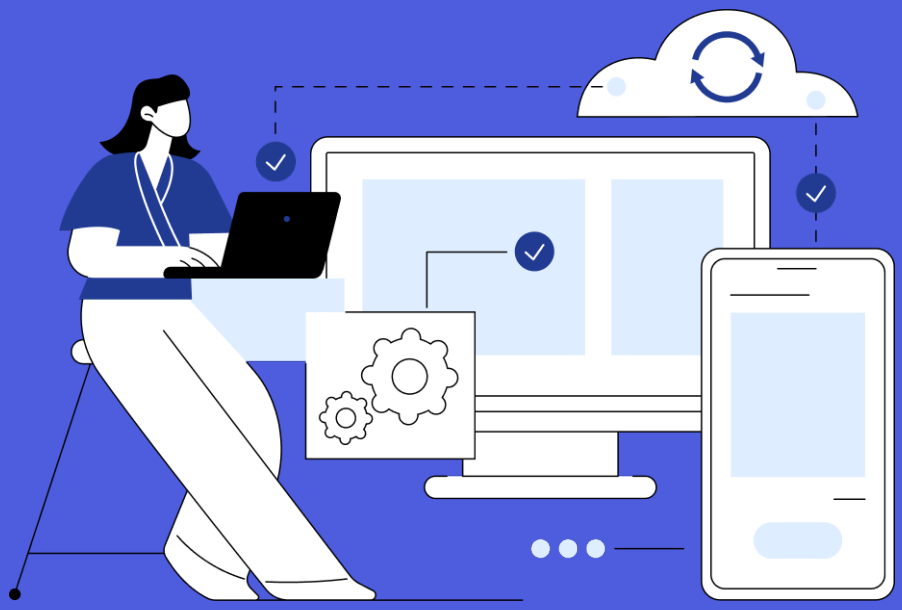

Enterprise Cloud Migration in Australia: Compliance & Readiness Checklist

For Australian Enterprises | 2026 Edition

Actionable checkpoints across strategy, compliance, architecture, security, FinOps and modernisation

Aligned with: APRA CPS 234 | Privacy Act 1988 (Cth) | ASD Essential Eight | APS Cloud Policy 2026 | AWS Well-Architected

Delivered by Appinventiv — AWS Advanced Tier Partner | Approved ICT Supplier — All Levels of Australian Government | APAC's High-Growth Companies by Statista & FT for Three Consecutive Years

How to Use This Checklist

This checklist is structured across three phases of an enterprise cloud migration programme. Each item includes a brief explanation of why it matters and what good looks like — not just what to do, but what to consider when you do it.

It is designed for CIOs, CTOs, Cloud Architects, IT Programme Managers and Compliance Leads in Australian enterprises planning or executing a cloud migration programme. It reflects the compliance obligations specific to Australia, including APRA CPS 234, the Privacy Act 1988 and its 2024 amendments, the ASD Essential Eight, and the APS Whole-of-Government Cloud Computing Policy effective 1 July 2026.

PHASE 1 PRE-MIGRATION

This phase covers everything that must be in place before any workload moves to cloud. The quality of pre-migration work is the single greatest predictor of programme success. Organisations that rush this phase consistently overrun on time and cost. Those that invest in it properly run smoother, faster migration waves with fewer surprises.

	A. Business Case & Stakeholder Alignment
☐	Define the business case with measurable outcomes
☐	Identify and align all executive sponsors
☐	Map all stakeholders and their migration concerns
☐	Establish a Cloud Migration Programme Office (CMPO)
☐	Define success criteria and decision gates

	B. Application Portfolio Discovery & Assessment
☐	Catalogue every application, database and integration
☐	Map all application dependencies and data flows
☐	Classify all data by sensitivity and regulatory category
☐	Apply the 7Rs framework to every workload
☐	Identify candidates for decommissioning before migration
☐	Assess current performance baselines for all critical systems
☐	Document current licensing models for all software

	C. Compliance & Regulatory Readiness
☐	Conduct a full Privacy Act and APRA compliance gap analysis
☐	Confirm data residency requirements for all workloads
☐	Review APRA CPS 234 third-party risk management obligations
☐	Assess ASD Essential Eight compliance posture
☐	Check obligations under the APS Whole-of-Government Cloud Policy (effective 1 July 2026)

☐	Review state-level privacy obligations where applicable
☐	Engage your legal and risk teams in architecture decisions
D. Cloud Architecture & Landing Zone Design	
☐	Select your target cloud platform(s) and deployment model
☐	Design the cloud landing zone before migration begins
☐	Define Identity and Access Management (IAM) architecture
☐	Establish network architecture: segmentation, peering and connectivity
☐	Define encryption standards for data at rest and in transit
☐	Select and configure logging, monitoring and observability tooling
☐	Design the FinOps governance model
E. Migration Planning & Wave Sequencing	
☐	Create a prioritised migration wave plan
☐	Build a detailed cutover runbook for each migration wave
☐	Define rollback criteria and rollback procedures
☐	Establish a parallel-running window for each critical system
☐	Plan and budget for staff training and capability uplift
☐	Agree the communications and change management plan

Appinventiv Insight

Appinventiv's cloud migration consulting team typically spends the following time in Phase 1 discovery and design:

- 4–8 weeks for mid-market programmes.
- 8–16 weeks for large enterprise or government engagements.

PHASE 2 DURING MIGRATION

Execution, Validation, Security & Change Management

This phase covers migration execution from landing zone build-out through to production go-live of each workload wave. The focus shifts from planning to delivery but governance discipline must intensify, not relax. The compliance risk is highest when data exists in both environments simultaneously, and the most damaging production incidents occur in programmes that deprioritised testing in favour of speed.

	F. Cloud Environment Build & Validation
☐	Provision and validate the cloud landing zone in non-production
☐	Run a security configuration audit against your baseline controls
☐	Validate data residency enforcement mechanisms
☐	Test IAM policies and least-privilege access controls
☐	Validate backup, recovery and disaster recovery configurations
	G. Workload Migration Execution
☐	Execute Wave 1 migration with low-risk workloads
☐	Conduct post-migration functional testing for every migrated workload
☐	Validate performance against pre-migration baselines
☐	Verify all integrations and API connections are functioning
☐	Confirm logging and monitoring is capturing all expected events
☐	Conduct data validation and reconciliation checks
☐	Complete and sign off the post-migration validation checklist for each wave
	H. Security, Compliance & Governance During Migration
☐	Maintain consistent access controls across both environments during parallel running

☐	Ensure encryption is active on all data in transit during migration
☐	Log and retain all migration activity for audit purposes
☐	Conduct vulnerability scans on migrated workloads before production go-live
☐	Test incident response procedures in the cloud environment

I. FinOps & Cost Management During Migration

☐	Monitor cloud spend daily during active migration waves
☐	Tag all provisioned resources from day one
☐	Review parallel-running costs and plan decommissioning timelines
☐	Track migration programme costs against budget weekly

J. Communication & Change Management During Migration

☐	Communicate each migration wave schedule to affected business users
☐	Run a hypercare support model for the first two weeks post-cutover
☐	Conduct a post-wave retrospective after each migration wave

Appinventiv Insight

Appinventiv's cloud execution team typically spends the following time per migration wave during Phase 2 execution:

- 2–4 weeks per wave for mid-market programmes.
- 6–8 weeks per wave for highly regulated enterprise or government workloads.

PHASE 3 POST-MIGRATION

Optimisation, Governance, FinOps & Continuos Modernisation

Migration is an event. Running cloud infrastructure well is an ongoing discipline. Organisations that invest in execution but neglect optimisation and governance typically see cloud costs increase unpredictably, security configuration drift over time, and performance degrade as usage evolves. This phase never truly ends — it matures into standard operating practice.

K. Performance Optimisation & Rightsizing	
☐	**Rightsize all cloud instances within 30 days of go-live**
☐	**Implement auto-scaling for variable-load workloads**
☐	**Review and optimise storage configurations**
☐	**Optimise data transfer and egress costs**
☐	**Conduct a 90-day performance review against pre-migration baselines**
L. FinOps Maturity & Cost Governance	
☐	**Purchase Reserved Instances or Savings Plans for stable workloads**
☐	**Implement a cloud cost anomaly detection system**
☐	**Establish monthly FinOps review meetings with cost centre owners**
☐	**Review and eliminate idle or unused resources quarterly**
☐	**Publish a cloud cost efficiency scorecard to leadership**
M. Ongoing Security, Compliance & Governance	
☐	**Decommission source environments promptly after validation**
☐	**Schedule an annual APRA CPS 234 cloud security control review**
☐	**Maintain continuous compliance monitoring with cloud-native tooling**
☐	**Conduct quarterly access reviews and privilege audits**

☐	Test disaster recovery and failover procedures every six months
☐	Review and update data residency controls after any platform change
☐	Maintain an up-to-date cloud asset inventory and CMDB

N. Continuous Modernisation & Cloud Maturity

☐	Establish a Cloud Centre of Excellence (CCoE) or Platform Engineering team
☐	Adopt Infrastructure as Code for all new cloud provisioning
☐	Implement CI/CD pipelines for application deployment
☐	Plan and schedule refactoring for high-value Rehost workloads
☐	Build your AI/ML cloud architecture roadmap
☐	Conduct an annual cloud architecture review (AWS Well-Architected / Azure Well-Architected Framework)

O. Vendor & Partner Management Post-Migration

☐	Review and renegotiate cloud provider enterprise agreements annually
☐	Assess cloud provider service level agreements against business continuity obligations
☐	Document and test cloud exit procedures annually

Appinventiv Insight

Appinventiv's FinOps and platform engineering teams typically structure Phase 3 optimisation and modernisation into:

- Immediate post-go-live rightsizing
- Ongoing continuous modernisation

About Appinventiv

For Australian Enterprises | 2026 Edition

Appinventiv is a digital product engineering company with a dedicated cloud practice serving Australian enterprises across financial services, healthcare, logistics, retail, and government. With over 1,600 technology professionals and on-the-ground delivery capability in Sydney, Melbourne and Brisbane, we bring both the technical depth and the Australian regulatory knowledge that enterprise cloud migration programmes require.

Our credentials:	What we deliver:
AWS Advanced Tier Partner with triple competency recognition in DevOps, Migration, and Well-Architected Review	Cloud migration strategy and workload assessment using the 7Rs framework
Approved ICT Supplier — All Levels of Australian Government, including Queensland Government Local Buy programme	Cloud landing zone design aligned with APRA CPS 234, Privacy Act and ASD Essential Eight
Deloitte Technology Fast 50 winner — 2023 and 2024	Wave-based migration execution with rollback assurance and hypercare support
APAC High-Growth Company for Three Consecutive Years by Statista and Financial Times	Application modernisation: containerisation, microservices, DevSecOps, IaC
	FinOps practice integration from programme day one

Ready to plan your cloud migration programme?

Speak with our cloud architects; no obligation, no sales pitch. Just clarity on your programme.

Request Your Migration Readiness Review

What the Readiness Review Covers

- Workload discovery and 7Rs classification for your top 20 applications
- Compliance gap analysis against APRA CPS 234, the Privacy Act and ASD Essential Eight
- Cloud architecture options and landing zone design recommendations
- Indicative programme budget and timeline
- Migration wave sequencing with risk and dependency mapping

Available for Australian enterprises across Sydney, Melbourne, Brisbane, Perth, Darwin and remote delivery.

Disclaimer: Content is provided for informational purposes and does not constitute legal or compliance advice. Consult a qualified adviser for obligations specific to your organisation.