Cloud Governance and Threat Assessment

A Compliance-Driven Security Evaluation

By Om Shah

University of Technology Sydney

Due: 1 September 2025

Table of Contents

Contents

Executive Summary

This report evaluates the security feasibility of migrating selected workloads from on-premises infrastructure to Amazon Web Services (AWS). Using ACSC guidance, the AWS Well-Architected Framework and MITRE ATT&CK for Cloud, we assessed threats, mapped responsibilities under the AWS Shared Responsibility Model, and aligned controls to Australian privacy obligations. The conclusion is that migration is feasible if governance guardrails are implemented and operated to a defined standard, with clear accountability for identities, data protection, monitoring and recovery ***(Amazon Web Services, n.d.a)***.

The main risks are wrong access settings, data leaks from public endpoints or storage, weak logging that makes it hard to detect issues, poor key management, and problems when data is handled overseas. To manage these risks, we suggest using separate AWS accounts with clear rules, enforcing MFA and only giving people necessary access, encrypting all data with customer-managed keys, keeping networks private with controlled traffic and VPC endpoints, protecting public apps with WAF and Shield, and storing all logs in one place with CloudTrail, Config checks, and continuous monitoring ***(Security Hub, GuardDuty, Macie).*** Business continuity uses multi-AZ designs to keep services running and, when needed, pilot-light or warm-standby disaster recovery to restore systems. Legal compliance is supported by privacy impact assessments, keeping proper evidence, and using contract terms that meet the Notifiable Data Breaches scheme and APP 8 cross-border rules ***(Office of the Australian Information Commissioner, n.d.a; Office of the Australian Information Commissioner, n.d.b)***.

We suggest moving to the cloud in phases: start with the foundations, then migrate low-risk workloads, and finally critical workloads. Each step should only commence once controls are proven to work and practice runs are successful. The next step is to approve Phase 1, which focuses on building the foundations along with staff training and assurance activities.

Introduction

Many organisations are shifting from on-premises data centres to AWS to scale faster, save money, and deliver services efficiently. In the cloud, security is a shared responsibility. AWS secures the physical facilities, hardware, and core services, while we are responsible for securing what we set up and manage, such as data, identities, applications, and network settings. Figure 1 shows this split, which is the basis for the approach in this report. ***(AWS, n.d.a)***.

We map that split of duties to Australian law, including the Privacy Act 1988 and the Notifiable Data Breaches, or NDB, scheme, with a focus on keeping data in Australia where required and managing any cross-border disclosure under APP 8 ***(Commonwealth of Australia, 1988; OAIC, n.d.a; OAIC, n.d.b)***. We identify likely threats using MITRE ATT&CK for Cloud and guidance from the Australian Cyber Security Centre (ACSC). Both emphasise that the organisation remains accountable for data security **(MITRE, n.d.; ACSC, 2021).** We then use the Security Pillar of the AWS Well-Architected Framework to set a safe, phased migration path and show how security will be measured and improved over time ***(AWS, n.d.b).***

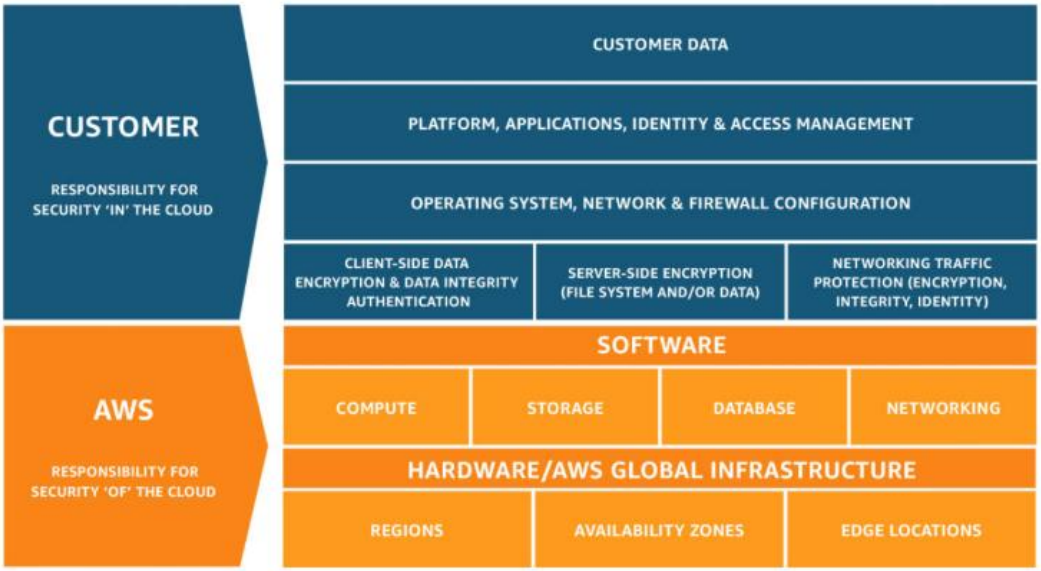

Figure 1- AWS shared responsibility model ***(AWS, n.d.a).***

Research Objectives

This assessment will baseline cloud risk, map responsibilities, and align legal obligations to a practical control set so management can decide on a secure, staged AWS migration. It focuses on evidence that can be measured and audited ***(AWS, n.d.a; AWS, n.d.b)***. To achieve this, the assessment will:

- Quantify inherent and residual risk via a risk register and heatmap.
- Map controls to the AWS Shared Responsibility Model and produce a RACI ***(AWS, n.d.a)***.
- Identify applicable obligations: Privacy Act 1988, Notifiable Data Breaches, and cross-border exposure under the Australian Privacy Principles ***(Commonwealth of Australia, 1988; OAIC, n.d.a; OAIC, n.d.b)***.
- Define a reference security architecture and guardrails aligned to the Well-Architected Security Pillar ***(AWS, n.d.b)***.
- Specify Security SLA requirements: incident notification windows, evidence handling, audit rights, data residency and exit.
- Set BCDR targets (RTO/RPO), choose patterns, and outline test scenarios.
- Draft a migration roadmap with milestones, cost levers and success metrics.

Scope of Works

In Scope

The evaluation sets up a secure foundation across several AWS accounts, all governed from one place. Staff sign in through the existing company login with multi-factor checks and only get the minimum access they need. Networks are private by default, and only approved traffic can leave. All data is encrypted automatically, with keys managed by us, we can add hardware-level protection for higher-risk material. Logs and configuration checks flow into a single dashboard so we can spot issues quickly and prove compliance. Applications run using a mix of virtual machines, containers and

serverless services, and data is stored in managed storage and databases. Backups run automatically and are tamper-proof ***(AWS, n.d.f)***.

We handle customer and staff personal information, sensitive business records and security logs. Sydney (ap-southeast-2) is our primary region, and we will assess a second region for disaster recovery and data sovereignty needs. The design connects privately to our offices and data centre, integrates with single sign-on and our build pipelines, and follows well-defined processes for incident response, change control, patching, and compliance. These controls are defined as code and reported on regularly so we can show who did what, when, and that the system stays within policy.

Out of Scope

We are not assessing unrelated third-party SaaS, the physical security of our data centres beyond the private links into AWS, detailed comparisons between cloud vendors, or product features that do not affect security, compliance, or resilience.

Assumptions

We will handle sensitive data. Everyone signs in with multi-factor authentication. Encryption keys and logs are managed in one place. An emergency “break-glass” admin path exists. Logs are kept long enough and time-stamped accurately to support investigations.

Constraints

Privacy and data-location rules may limit which AWS Regions we can use and whether we can copy data across borders. Existing contracts, licences, network design and team skills will influence the order and pace of work. Recovery targets for time and data loss must fit the budget and the time available for testing.

Methodology

Grounded in authoritative guidance, we apply a practical, evidence-led method that draws on the Australian Cyber Security Centre’s cloud security advice, the AWS Well-Architected Security Pillar, the OAIC’s Privacy Act and Notifiable Data Breaches guidance including APP 8, and the MITRE

ATT&CK framework for cloud ***(ACSC, 2021; AWS, n.d.b; OAIC, n.d.a; OAIC n.d.b; MITRE, n.d.)***. We start by listing every system and mapping how data moves between them and then identify the realistic ways someone could attack those cloud systems. For each risk, we rate how likely it is and how serious the impact would be and choose controls to stop attacks, to spot them quickly, and to recover if something goes wrong. We then check that this works in practice by using AWS Config to automatically verify settings, GuardDuty to detect suspicious activity, Security Hub to bring all alerts into one place, and regular tabletop exercises to practise incident response and keep the business running.

Current-Target Architecture on AWS

We manage multiple AWS accounts through a central hub using AWS Organisations and Control Tower, applying service control policies to block unsafe actions before they occur. The network is private by default, with workloads running inside VPCs that use private subnets and VPC endpoints for secure service access, while outbound traffic is restricted through controlled egress paths. Public-facing applications are routed through an Application Load Balancer and further protected by AWS WAF, with Shield Advanced providing additional resilience against DDoS attacks.

Data is encrypted both at rest and in transit using AWS KMS keys that we manage, supported by key policies that separate platform and security responsibilities. Logs and monitoring are centralised: an organisation-level CloudTrail sends records to a locked archive, AWS Config enforces compliance against conformance packs, and GuardDuty, Detective and Security Hub provide continuous detection with a unified view of findings. Secrets Manager secures credentials, while Macie identifies and classifies personal information to reduce the risk of exposure ***(AWS, n.d.c; AWS, n.d.d; AWS, n.d.e)***.

We design for resilience. Multi-AZ keeps services available during failures. AWS Backup creates automatic, tamper-proof backups with Vault Lock. Where it is justified, we add a second

Region for recovery. This target state follows the AWS Well-Architected Security guidance and makes shared responsibilities clear ***(AWS, n.d.a; AWS, n.d.b)***.

Threats and Risk Analysis

Identity and access are the biggest cloud risk. If roles are set up incorrectly, if people have more permissions than they need, or if multi-factor authentication is missing, attackers can gain higher privileges and move between systems. We reduce this by using least-privilege roles, conditional IAM policies, regular access reviews, service control policies that block risky actions, and single sign-on with multi-factor authentication ***(MITRE, n.d.; AWS, n.d.b)***.

Accidental data exposure is the next major issue. Public endpoints or wrongly configured storage can leak information. We lower this risk by keeping networks private, using VPC endpoints for service access, controlling egress, and protecting internet sites with AWS WAF and Shield. We also use Amazon Macie to find personal information that may be at risk so it can be fixed quickly ***(AWS, n.d.b; AWS, n.d.e)***.

Weak logging and forensics make it hard to detect breaches and to meet legal duties. We turn on CloudTrail at the organisation level, enforce settings with AWS Config and conformance packs, and keep logs in an immutable archive using S3 Object Lock. Security Hub provides a baseline view across accounts. These measures help us gather evidence and meet Notifiable Data Breaches assessment and notification steps if needed ***(OAIC, n.d.a; AWS, n.d.b; AWS, n.d.g)***.

Key management mistakes and poor data lifecycle controls can cause data loss or unlawful disclosure. We use customer managed KMS keys with clear ownership, separation of duties, rotation, and safe deletion processes. We also apply strict permissions to sensitive actions like scheduling key deletion and use lifecycle policies to control retention ***(AWS, n.d.b)***.

Availability threats include denial-of-service, noisy neighbours and ransomware that targets backups. We protect availability with Multi-AZ designs and, where justified, a second Region for

recovery. We create automatic, tamper-proof backups with AWS Backup and Vault Lock, rehearse restores with runbooks, and use WAF and Shield to reduce both volumetric and application-layer attacks ***(AWS, n.d.b; AWS, n.d.h)***.

There are also risks when data crosses borders or when overseas support teams can access it. We choose Regions carefully, document data flows, encrypt with our own KMS keys and use contract terms to control access. If a breach involves personal information, the NDB scheme and APP 8 guide our assessment, notification, and cross-border due diligence ***(OAIC, n.d.a; OAIC, n.d.b)***.

We record the remaining risk for each item in a register with an owner, treatment, and review date. Figure 2 shows our risk heatmap, and Table 1 maps each named risk to a cell on the matrix. This highlights identity misconfiguration and public data exposure as high-impact, medium-likelihood priorities, with logging, key management, and cross-border exposure following behind.

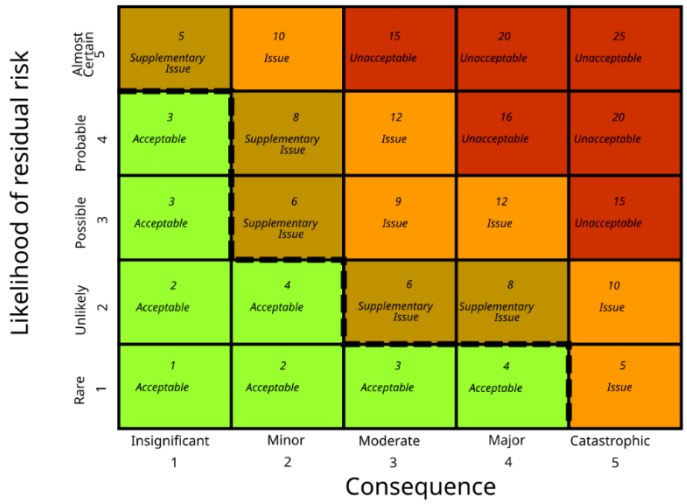

Figure 2 - Risk heatmap showing likelihood and consequence of residual risk. ***(Wlofab, 2013)***

Table 1 - Risk mapping of identified cloud threats against likelihood and consequence scores.

Risk	Likelihood (1-5)	Consequence (1-5)	Why
IAM misconfiguration	4	5	Privilege escalation and lateral movement are called out as the biggest risk
Public data exposure	4	5	Public endpoints or storage leaks are a major issue in your analysis
Weak logging and forensics	3	4	Hinders breach detection and NDB assessment, medium to high impact
Key management weaknesses	3	4	Loss or unlawful disclosure if keys are mishandled
Cross-border exposure	3	5	High impact due to APP 8 and NDB, likelihood lower within current scope

Legal, Policy and Regulatory Requirements

The move to AWS must comply with Australia's privacy law and keep evidence that will stand up in an investigation. The Commonwealth Privacy Act 1988 sets the baseline. The Australian Privacy Principles, or APPs, require organisations to take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access or disclosure under APP 11. The OAIC's Guide to securing personal information explains what reasonable steps look like in practice, including access controls, encryption, monitoring, retention, and secure disposal ***(OAIC, n.d.)***.

If a suspected eligible data breach occurs, the Notifiable Data Breaches scheme, or NDB, requires a prompt assessment. Entities must take reasonable steps to complete that assessment within 30 days of becoming aware, then notify the OAIC and affected individuals if serious harm is likely ***(OAIC, n.d.)***. The architecture therefore needs immutable logging, accurate time synchronisation and sound evidence preservation to support that assessment and any notification. We use organisation-level CloudTrail, a central log archive with S3 Object Lock, and Config conformance packs to demonstrate reasonable steps and maintain evidentiary integrity ***(AWS, n.d.g)***.

Cross-border disclosure is governed by APP 8. In most cases the Australian entity remains accountable for how an overseas recipient handles personal information. Before sending data offshore, entities must take reasonable steps to ensure the recipient will comply with the APPs, usually through enforceable contract terms, or rely on a permitted exception ***(OAIC, n.d.)***. In practice this drives careful Region selection such as the Sydney region ap-southeast-2, documented data flows, encryption with customer-managed keys, and tight contractual controls over any support access that may cross borders. Where overseas processing is unavoidable, privacy impact assessments and supplier due diligence are expected.

Where relevant, sector rules also apply. The Australian Prudential Regulation Authority, or APRA, expects compliance with CPS 234 for regulated entities, including security capability that matches the threat and timely incident notification to the regulator. The ACSC's Cloud Computing Security Considerations add due-diligence prompts, especially when vendors operate offshore. Together these sources shape policy guardrails, assurance activities and contract or service-level terms.

Governance, SLA and the Shared Responsibility Model

Governance keeps the migration on track by clarifying roles and demonstrating that they work in practice. Under the AWS Shared Responsibility Model, AWS secures the cloud infrastructure, while the organisation remains responsible for identities, data, configuration and monitoring within its services ***(AWS, n.d.a).*** The approach uses a multi-account landing zone with policy guardrails, overseen by a central team that manages identity, encryption keys, logging and outbound network access. Controls are defined as code and measured against configuration baselines with continuous detection aligned to the Well-Architected Security Pillar ***(AWS, n.d.b).*** A RACI then specifies who is responsible and accountable, and who is consulted and informed, across identity lifecycle, vulnerability management, incident response, and backup or recovery.

Security service level agreements align with Australian law and day-to-day operations. They set clear incident notification timeframes so we can complete a Notifiable Data Breaches assessment and notify the Office of the Australian Information Commissioner and affected people when required. They define audit and assurance using provider attestations and our configuration evidence. They set data residency in Sydney ap-southeast-2 and control any cross-border support access. They confirm that we own and manage our KMS keys and describe safe destruction. They specify log retention and evidence rules for investigations, availability targets with support response times, and an exit plan that covers data export, secure deletion and revoking certificates or keys ***(OAIC, n.d.a; AWS, n.d.a)***. We enforce these terms through internal policy, regular reviews, and tabletop exercises, and track any exceptions until they are closed.

Business Continuity and Disaster Recovery (BCDR) on AWS

Business continuity and disaster recovery set clear recovery time objectives, or RTOs, and recovery point objectives, or RPOs, for each business tier. We then choose patterns that meet those targets and prove they work. For high availability, workloads run across multiple Availability Zones with automatic failover. For disaster recovery, critical systems use pilot light or warm standby in a second Region. Lower criticality systems use backup and restore. Infrastructure is defined as code so it can be rebuilt in a predictable way. Data protection combines service snapshots with central backups using AWS Backup and Backup Vault Lock to keep copies immutable and retained as required.

Monitoring and procedures are part of recovery. CloudWatch raises alarms. CloudTrail at the organisation level and AWS Config baselines confirm the restored state meets policy. Regular game days and tabletop exercises test failover, check RTO and RPO timings, and exercise people, processes and tools. The design also covers dependencies such as DNS, identity, encryption keys, network connectivity and secrets so recovery steps run in the right order and with the right access. If we enable cross-Region replication, we must first recheck privacy and residency constraints and encrypt

with customer-managed keys to reduce exposure. This approach follows the AWS Well-Architected guidance for security and reliability and aligns with ACSC expectations for continuity in cloud environments ***(AWS, n.d.b; ACSC, 2021)***.

Recommendations and Roadmap

Adopt a phased migration plan that delivers value safely and predictably. Set clear entry and exit gates for each phase based on governance guardrails and operational readiness. Move to the next phase only after controls are implemented, tested, and documented.

Phase 1 foundations. Build the multi-account landing zone with service control policies. Federate identity with multi-factor authentication, or MFA, and keep an emergency break-glass path. Enforce encryption with customer managed KMS keys. Centralise logging with organisation-level CloudTrail and a locked S3 archive. Set configuration baselines and continuous detection with Config, GuardDuty, Security Hub and Macie ***(AWS, n.d.c; AWS, n.d.d; AWS, n.d.e)***. Tighten network egress and use private endpoints. Protect internet-facing services with WAF and Shield. Configure immutable backups and runbooks. Lift skills and rehearse incident response in a way that supports Notifiable Data Breaches assessment and notification ***(AWS, n.d.b; OAIC, n.d.a).***

Phase 2 low-risk workloads. Migrate non-critical services using infrastructure as code and mandatory tagging. Use pilot-light disaster recovery, or DR. Prove control effectiveness with conformance packs and detection coverage. Complete privacy impact assessments when data flows change ***(ACSC, 2021)***.

Phase 3 critical workloads. Move to warm standby or active where the business case supports it. Agree and embed service level agreement, or SLA, terms for notification, audit, residency, key ownership, and exit. Run red-team exercises and recovery game days.

Track outcomes using metrics such as Mean Time to Detect (MTTD), Mean Time to Recover (MTTR), configuration compliance rates, restore success rates, identity review completion, and cost

controls. This staged approach aligns with the AWS Well-Architected Framework for security and reliability while also supporting legal defensibility ***(AWS, n.d.b).***

Conclusion

A move to AWS is feasible if we put the right controls in place. We need strong governance, least-privilege access, encryption by default, tight egress controls, centralised and tamper-proof logging, and regular recovery tests. With a phased roadmap, clear responsibilities and contract terms that support privacy and breach notification, residual risk can stay within appetite while agility and resilience improve. The recommended path is to approve Phase 1 foundations now, then move each migration wave only after controls are proven and rehearsals show they work ***(OAIC, n.d.a; AWS, n.d.b)***.

References

Amazon Web Services. (n.d.a). *Shared responsibility model*. AWS. https://aws.amazon.com/compliance/shared-responsibility-model/

Amazon Web Services. (n.d.b). *Security pillar – AWS Well-Architected Framework*. AWS. https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

Amazon Web Services. (n.d.c). *Amazon GuardDuty*. AWS. https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

Amazon Web Services. (n.d.d). *AWS Security Hub*. AWS. https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

Amazon Web Services. (n.d.e). *Amazon Macie*. AWS. https://docs.aws.amazon.com/macie/latest/user/what-is-macie.html

Amazon Web Services. (n.d.f). *AWS Config conformance packs*. AWS. https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html

Amazon Web Services. (n.d.g). *Amazon S3 Object Lock*. AWS. https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html

Amazon Web Services. (n.d.h). *AWS Backup Vault Lock*. AWS. https://docs.aws.amazon.com/aws-backup/latest/devguide/vault-lock.html

Australian Cyber Security Centre. (2021). *Cloud computing security considerations*. Australian Government. https://www.cyber.gov.au/resources-business-and-government/maintaining-system-security/cloud-security/cloud-computing-security-considerations

Commonwealth of Australia. (1988). *Privacy Act 1988 (Cth).* https://www.legislation.gov.au/C2004A03712/latest

MITRE. (n.d.). *ATT&CK matrix for cloud*. MITRE. https://attack.mitre.org/matrices/enterprise/cloud/

Office of the Australian Information Commissioner. (n.d.a). *About the Notifiable Data Breaches scheme*. OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

Office of the Australian Information Commissioner. (n.d.b). *Chapter 8 - APP 8: Cross-border disclosure of personal information*. OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information

Office of the Australian Information Commissioner. (n.d.c). *Guide to securing personal information.* OAIC. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information

Wlofab. (2013). *Risk analysis chart* [Figure 2]. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Risk_Analysis_Chart.svg