# AWS User Guide to Financial Services Regulations & Guidelines in Australia

*April 2018*

**This paper has been archived**

---

**For the latest version of this paper, see**

https://d1.awsstatic.com/whitepapers/compliance/AWS_User_Guide_to_Financial_Services_Regulations_and_Guidelines_in_Australia.pdf

---



aws

[ Resource Guide ]

# Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

# Contents





# Abstract

This document provides information to assist financial services institutions in Australia that are regulated by the Australian Prudential Regulation Authority as they accelerate their use of Amazon Web Services' cloud services.

# Introduction

The Australian Prudential Regulation Authority (APRA) is the primary financial regulator in Australia. APRA oversees banks, credit unions, building societies, general insurance and reinsurance companies, life insurance, private health insurance, friendly societies, and most members of the superannuation industry (APRA regulated institutions or ARIs).

In July 2017, APRA updated Prudential Standard CPS 231 on "Outsourcing". CPS 231 requires ARIs to perform due diligence and apply sound governance and risk management practices to their outsourcing of a material business activity, including via their use of cloud services. While the use of Amazon Web Services' (AWS) cloud services by ARIs substantially pre-dates the update to CPS 231, AWS welcomes the increased clarity and guidance provided by APRA.

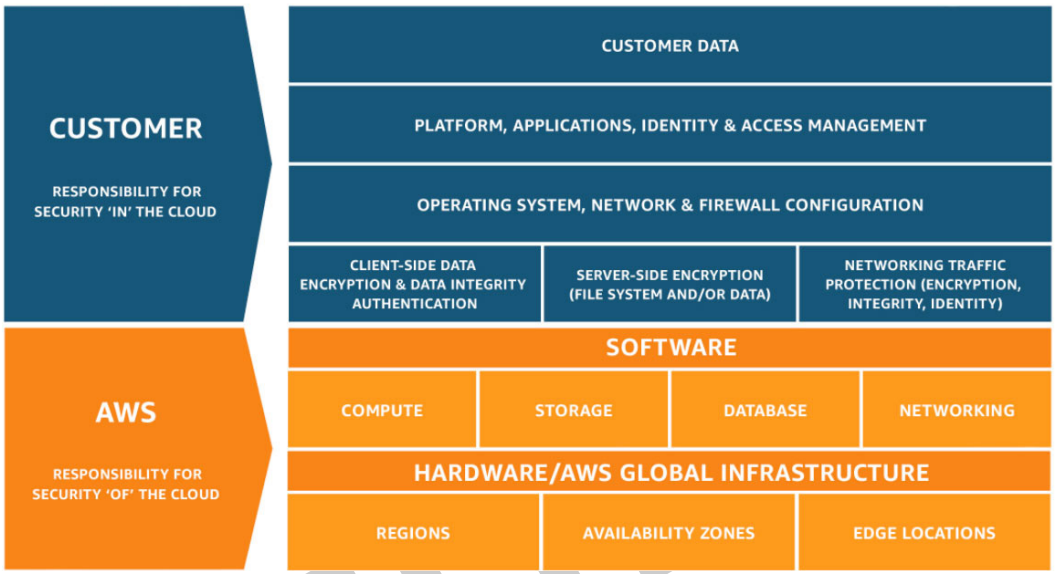
The following sections provide considerations for ARIs as they assess their responsibilities with regards to the following guidelines and requirements:

- **CPS 231 "Outsourcing":** This Prudential Standard states APRA's requirements relating to the risk management of outsourcing arrangements for material business activities.
- **CPG 234 "Management of Security Risk in Information and Technology":** This Prudential Practice Guide provides APRA's guidance to ARIs on safeguarding IT assets.
- **APRA "Information Paper on Outsourcing Involving Shared Computing Services (Including Cloud)":** This paper contains APRA's guidance for ARI's when using cloud services for material business activities.

Taken together, ARIs can use this information to commence their due diligence and assess how to implement an appropriate information security, risk management and governance program for their use of AWS.

# Security and Shared Responsibility

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS infrastructure complies with global and regional regulatory requirements and best practices, but security in the cloud is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site data centre.




**Shared Responsibility Model**

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles. AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

## Security in the Cloud

Customers are responsible for their security in the cloud. Much like a traditional data centre, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

It is important to note that when using AWS services, customers maintain control over their content and are

responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that are used with the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

## Security of the Cloud

In order to provide Security of the Cloud, AWS continuously audits its environments. The infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that can be implemented, and to better assist customers with managing their control environment.
- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with information regarding the policies, processes, and controls established and operated by AWS. Customers can use this information to perform their control evaluation and verification procedures, as required under the applicable compliance standard.
- **Monitor**, through the use of thousands of security control requirements, that AWS maintains compliance with global standards and best practices.

# AWS Compliance Assurance Programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads, however the following are of particular importance to ARIs:

**ISO 27001** – ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

**ISO 27017** – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

**ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

**ISO 9001** - ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

**PCI DSS Level 1** - The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council. PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

**SOC** – AWS System & Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, see the SOC Compliance webpage. There are three types of AWS SOC Reports:

- **SOC 1:** Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting as well as information for assessment and opinion of the effectiveness of internal controls over financial reporting (ICOFR).
- **SOC 2:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
- **SOC 3:** Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality without disclosing AWS internal information.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see the AWS Assurance Programs webpage. For information about general AWS security controls and service-specific security, see the Amazon Web Services: Overview of Security Processes whitepaper.



# AWS Artifact

Customers can use AWS Artifact to review and download reports and details about more than 2,500 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports and certifications from accreditation bodies across geographies and compliance verticals.

# AWS Regions

The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world that is made up of multiple Availability Zones. Availability Zones consist of one or more discrete data centres that are housed in separate facilities, each with redundant power, networking, and connectivity. These Availability Zones offer customers the ability to operate production applications and databases at higher availability, fault tolerance, and scalability than would be possible from a single data centre. The AWS Cloud operates 54 Availability Zones within 18 AWS Regions around the world. For current information on AWS Regions and Availability Zones, see https://aws.amazon.com/about-aws/global-infrastructure/.

AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic requirements. For example, AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) Region and store their content on shore in Australia, if this is their preferred location. If the customer makes this choice, their content will be located in Australia unless the customer chooses to move that content.

The AWS Asia Pacific (Sydney) Region is designed and built to meet rigorous compliance standards globally, providing high levels of security for all AWS customers. As with every AWS Region, the Asia Pacific (Sydney) Region is compliant with applicable national and global data protection laws.

# CPS 231 "Outsourcing"

CPS 231 outlines APRA's requirements for ARIs who plan to outsource material business activities, including via the use of cloud services. "Outsourcing" is defined as when an ARI engages another party, including a related body corporate, to perform on a continuing basis a business activity that either is, or could be, undertaken by the ARI. A "material business activity" is an activity that, if disrupted, could have a significant impact on the ARI or its ability to manage risks effectively.

CPS 231 requires that all outsourcing arrangements involving material business activities be subject to appropriate due diligence, approval and ongoing monitoring. All risks arising from this arrangement must be appropriately managed by the ARI to ensure it is able to meet its financial and service obligations. Key requirements of CPS 231 include that an ARI must:

- Have an outsourcing policy, approved by the ARI's board, relating to outsourcing of material business activities
- Have sufficient monitoring processes in place to manage the outsourcing of material business activities
- Have a legally binding outsourcing agreement in place with third parties for any outsourcing of material business activities, unless otherwise agreed by APRA
- Consult with APRA prior to entering into outsourcing agreements for material business activities where the outsourcing service provider conducts their activities outside Australia
- Notify APRA after entering into outsourcing agreements to outsource material business activities.

A full analysis of CPS 231 is beyond the scope of this document. However, the following sections address the considerations in CPS 231 that most frequently arise in interactions with ARIs.

## Outsourcing policy

Paragraphs 23 to 25 of CPS231 outline that an ARI must have an outsourcing policy approved by its board. This outsourcing policy must have sufficient monitoring processes in place, demonstrate the ARI's assessment of its proposed third party outsourcing arrangements, contain a legally binding outsourcing agreement with the third party outsourcer and provide for notification to APRA once the outsourcing agreement has been entered into.

AWS considers the development of an ARI's outsourcing policy as an action for the ARI to independently complete.

## Assessment of outsourcing options

Paragraph 26 of CPS 231 defines APRA's requirements when an ARI is assessing whether to outsource a material business activity. The following table includes considerations for components of paragraph 26 of CPS 231.

| Due Diligence Requirement | Customer Considerations |
|---|---|
| **26.(a) prepared a business case for outsourcing the material business activity** | AWS considers this an action for the ARI to independently complete. |
| **26.(b) undertaken a tender or other selection process for selecting the service provider** | AWS considers this an action for the ARI to independently complete. |
| **26.(c) undertaken a due diligence review of the chosen service provider, including the ability of the service provider to conduct the business activity on an ongoing basis** | Since 2006, AWS has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing us to provide new services that help millions of active customers.<br><br>The financial statements of Amazon.com Inc. include AWS's sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website.<br><br>Amazon.com Inc's Form 10-K filing is available at Amazon's Investor Relations website or the website of the US Securities and Exchange Commission, and includes details of legal proceedings involving Amazon.com, Inc., AWS, and other affiliates.<br><br>AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS.<br><br>AWS performs a continuous risk assessment process to identify, evaluate and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months.<br><br>Please refer to the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001, ISO 27017.<br><br>Amazon.com Inc. has a Code of Business Conduct and Ethics, available at Amazon's Investor Relations website, which covers issues including, among other things, compliance with laws, conflicts of interest, bribery, discrimination and harassment, health and safety, recordkeeping and financial integrity. |

| Due Diligence Requirement | Customer Considerations |
|---|---|
| **26.(d) involved the Board of the ARI, Board committee of the ARI, or senior manager of the ARI with delegated authority from the Board, in approving the agreement** | AWS considers this an action for the ARI to independently complete. |
| **26.(e) considered all the matters outlined in CPS 231 paragraph 29, that must, at a minimum, be included in the outsourcing agreement itself** | AWS customers have the option to enrol in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. AWS also provides an introductory guide to help ARIs assess the AWS Enterprise Agreement against CPS 231. For more information about AWS Enterprise Agreements, contact your AWS representative. |
| **26.(f) established procedures for monitoring performance under the outsourcing agreement on a continuing basis** | AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment. To learn more about each of the audit programs leveraged by AWS, see the AWS Assurance Programs webpage,<br><br>Compliance reports from these assessments are made available via AWS Artifact to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.<br><br>The AWS Service Health Dashboard provides up-to-the-minute information on the general availability of the services. The AWS Personal Health Dashboard gives customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and provides proactive notification to help customers plan for scheduled activities. |
| **26.(g) addressed the renewal process for outsourcing agreements and how the renewal will be conducted** | AWS agreements for use of the AWS services, including the AWS Customer Agreement, continue indefinitely until terminated by either party. |
| **26.(h) developed contingency plans that would enable the outsourced business activity to be provided by an alternative service provider or brought in-house if required** | Customers manage access to their content and to AWS services and resources, including the ability to import and export data. AWS provides services such as AWS Import/Export and AWS Snowball to transfer large amounts of data into and out of AWS using physical storage appliances. For more information, see https://aws.amazon.com/products/storage/.<br><br>Additionally, AWS offers AWS Database Migration Service, a web service customers can use to migrate a database from an AWS service to an on-premises database. |

## The outsourcing agreement

Paragraph 28 of CPS 231 requires each ARI have a legally binding agreement in place with the outsourcing service provider for any outsourcing of material business activities.

Paragraphs 29 to 30 of CPS 231 state APRA's requirements that outsourcing agreements address, at a minimum, the scope of the arrangement and services to be supplied; commencement and end dates; review provisions; pricing and fee structure; service levels and performance requirements; the form in which data is to be kept and clear provisions identifying ownership and control of data; reporting requirements (including content and frequency of reporting); audit and monitoring procedures; business continuity management; confidentiality; privacy and security of information; default arrangement and termination provisions; dispute resolution arrangements; liability and indemnity; sub-contracting; insurance; and offshoring arrangements (where applicable).

Paragraphs 34 to 36 of CPS 231 require that the outsourcing agreement address APRA's access to documentation and information related to the outsourcing agreement.

AWS customers have the option to enrol in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. AWS also provides an introductory guide to help ARIs assess the AWS Enterprise Agreement against CPS 231. For more information about AWS Enterprise Agreements, contact your AWS representative.

## Notification requirement

Paragraph 37 of CPS 231 requires ARIs to notify APRA as soon as possible on execution of an outsourcing agreement, and in any event no later than 20 business days. This notification must include a summary of key risks involved in the outsourcing agreement and risk mitigation strategies put in place by the ARI to address these risks.

AWS considers the ARI's notification to APRA as an action for the ARI to independently complete.

# CPG 234 "Management of Security Risk in Information and Information Technology"

CPG 234 "Management of Security Risk in Information and Information Technology" (CPG 234) provides APRA's guidance on particular areas to assist ARIs in the management of security risk in information and information technology (IT). CPG 234 does not create enforceable requirements on an ARI but addresses areas where APRA identifies weaknesses as part of its ongoing supervisory activities.

CPG 234 sets out risk management principles and best practice standards to guide ARIs in the following areas:

- Defining and classifying IT security risk
- Guidance on the structure and content of an IT security risk management framework

- User awareness
- Access control
- IT asset life-cycle management controls
- Monitoring and incident management
- IT security reporting and metrics
- IT security assurance

AWS has produced an AWS CPG 234 Workbook that documents relevant AWS controls for each of the CPG 234 guidelines. This Workbook covers the 8 sections and 6 appendixes documented within CPG 234 by APRA, and where AWS can provide information as part of the shared responsibility model, that information is mapped against the relevant section of CPG 234.

The following sample depicts part of the AWS response to CPG 234's "Access Control" section:

| ID | Guideline | Responsibility | AWS Response | Reference |
|---|---|---|---|---|
| **40** | Identification and authentication techniques<br><br>A regulated institution would normally take appropriate measures to identify and authenticate users or IT assets. The required strength of authentication would normally be commensurate with risk. | Shared | AWS controls access to systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. Remote access requires multi-factor authentication and the number of unsuccessful log-on attempts is limited. All remote administrative access attempts are logged, and the logs are reviewed by the Security team for unauthorized attempts or suspicious activity. If suspicious activity is detected, the incident response procedures are initiated.<br><br>AWS has implemented a session lock out policy that is systematically enforced. The information systems implement a session lock after a period of inactivity, as well as in the case of multiple log-in attempts, and limits the number of concurrent sessions that may exist. The session lock is retained until established identification and authentication procedures are performed. | PCI 3.2<br><br>ISO 27001<br><br>ISO 27017<br><br>ISO 27018 HIPAA<br><br>NIST 800-53 SOC 2 COMMON CRITERIA<br><br>SOC 1 & 2 CONTROLS |

| ID | Guideline | Responsibility | AWS Response | Reference |
|---|---|---|---|---|
| **41** | Common techniques for increasing the strength of identification and authentication include the use of strong password techniques (i.e. increased length, complexity, re-use limitations and frequency of change) and increasing the number and/or type of authentication factors used. Authentication factors include something a person knows, has and is. | Shared | Internal AWS users are required to change their passwords every 90 days. While users are allowed to select and change their own passwords, passwords must adhere to the AWS Password Policy. Requirements include, but are not limited to, a minimum password length, the inclusion of a mix of character types, not using a similar to a recently used password, and not using common words.<br><br>Internal AWS passwords are not transmitted or stored in an unencrypted form, or displayed in clear-text on the screen when being entered. Passwords associated with individual accounts are not shared with anyone or embedded in code, configuration files, batch files, scripts, or any other mechanism that is discoverable by anyone other than the owner of the account associated with the password. AWS does not permit temporary/emergency accounts or credentials.<br><br>In the event that an active or inactive user does not comply with the above stated policy, their account will be locked.<br><br>AWS requires multi-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations. | PCI 3.2<br><br>ISO 27001<br><br>ISO 27017<br><br>ISO 27018 HIPAA<br><br>NIST 800-53 SOC 1 & 2 CONTROLS |

ARIs may obtain a copy of the AWS CPG 234 Workbook via the AWS Artifact portal.

ARIs should review the AWS responses in the AWS APRA CPG 234 Workbook, and enrich them with the ARI's own company-wide controls. For example, Attachment D of CPG 234 covers "Secure software development" and recommends that ARIs implement secure software development lifecycle practices. This is a principle that will apply company-wide, not only to software that is developed for material business activities.

The AWS CPG 234 Workbook also helps ARIs to clearly consider whether, and how, to add extra or supplementary technology risk controls specific to line of businesses or application teams, or to meet the ARI's particular needs.

**Note:** It is important to appreciate the implications of the shared security responsibility model, and understand in each case which party is responsible for a particular control. Where AWS is responsible, the ARI should identify which of the AWS Assurance reports, certifications or attestations will be used to establish or assess that the control is operating.

# Information Paper on Outsourcing Involving Shared Computing Services (including Cloud)

Published in July 2015, APRA's "Information Paper on Outsourcing Involving Shared Computing Services (including Cloud)" (Information Paper) highlights recommendations and key principles that APRA states should be considered by an ARI when it contemplates using shared computing services, which include cloud services. The Information Paper excludes arrangements where IT assets are dedicated to a single ARI such as private cloud arrangements.

This section of the whitepaper focuses on Chapters 2 (APRA notification & consultation) and 3 (Risk management considerations) of the Information Paper.

## APRA notification and consultation

When using shared computing services, APRA states it is prudent for ARIs to only enter into arrangements where the risks are adequately understood and managed. This includes being able to demonstrate the following:

- Ability to continue operations and meet obligations following a loss of service
- Preservation of the quality (including security) of critical and/or sensitive data/information
- Compliance with legislative and prudential requirements
- Absence of jurisdictional, contractual or technical considerations which may inhibit APRA's ability to fulfil its duties as prudential regulator

APRA states ARIs should consult with APRA prior to entering into an outsourcing arrangement in the following scenarios:

1. The arrangement involves a material business activity that would be offshored
2. When the arrangement involves the use of shared computing services and involves *heightened inherent risks*

APRA states that environments where tenancy is also available to non-financial industry entities (such as public cloud) should be treated as if they have such heightened inherent risks.

ARIs are also encouraged to provide the following documentation to APRA to help facilitate the consultation process:

- Alignment to strategy, the business case, alternative options considered and rationale for the selected solution (including justification for additional risk exposures)
- IT assets in scope, categorized by sensitivity and criticality
- Impact on business processes, systems architecture, organization and operating model

- High-level risk and control assessments, risk profiles, plausible worst case scenarios and alignment to risk appetite and tolerances
- Services selected, products and parties involved and delivery location(s)
- Due diligence undertaken (including assurance obtained)
- When the detailed solution is designed and transition plans are in place:
    - Governance, project, risk management and assurance frameworks (initial and ongoing)
    - Operating model and security model to be applied, and associated roles / responsibilities of all parties (including handover and escalation points)
    - Alignment to regulatory standards and guidance
    - Architectural overview (including transitional states) for hardware, software and data stores
    - Detailed risk and control assessments, risk profiles and alignment to risk appetite and tolerances
    - Continuity of service strategy, including resilience, recovery and provider failure considerations
    - Organizational change management and transition plan
    - Project structure and schedule (including key stages, milestones and timeframes)

# Risk management considerations

Chapter 3 of the Information Paper outlines a non-exhaustive list of other considerations for assessment by ARIs when using shared computing services. The following table includes introductory information relevant to those considerations.

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| **Selection process** | A comprehensive due diligence process (including independent assessments and customer references) would normally be conducted to verify the maturity, adequacy and appropriateness of the provider and services selected (including the associated control environment), taking into account the intended usage of the shared computing service.<br><br>Post solution design, ARIs should conduct a risk assessment to consider:<br>• Ability to meet performance, capacity, security, resilience, recoverability and other business requirements;<br>• Adequacy of secure design principles and development practices utilized;<br>• Adequacy of processes to verify that software operates as intended within the shared computing service; and<br>• Critical and/or sensitive IT assets which are accessible from the shared computing service | Since 2006, AWS has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. AWS continues to grow and scale, allowing us to provide new services that help millions of active customers.<br><br>The financial statements of Amazon.com Inc. include AWS's sales and income, permitting assessment of its financial position and ability to service its debts and/or liabilities. These financial statements are available from the SEC or at Amazon's Investor Relations website.<br><br>A list of customer references and corresponding case studies can be found on the AWS Customer Success website.<br><br>Regarding the AWS corporate governance and culture, AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS.<br><br>AWS performs a continuous risk assessment process to identify, evaluate and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months.<br><br>Regarding the adequacy of secure design principles and development practices, customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Customers have complete control over which services they use and whom they empower to access their content and services, including what credentials will be required. Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS does not change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how security measures will be implemented in the cloud, in accordance with each customer's business needs. For example, if a higher availability architecture is required to protect customer content, the customer may add redundant systems, backups, locations, network uplinks, etc. to create a more resilient, high availability architecture. If restricted access to customer |

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| | | is required, AWS enables the customer to implement access rights management controls both on a systems level and through encryption on a data level.<br><br>Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS SOC 1, SOC 2 and SOC 3 reports, ISO 27001, ISO 27017 and ISO 27018 certifications and PCI DSS compliance reports. These reports and certifications are produced by independent third party auditors and attest to the design and operating effectiveness of AWS security controls. |
| **Risk assessments & security** | An ARI would normally conduct security and risk assessments, initially, periodically and on material change.<br><br>Comprehensive risk assessments typically include consideration of factors such as the nature of the service (including specific underlying arrangements, the provider and the location of the service), criticality and sensitivity of the IT assets involved, the transition process (delivery risk), and the target operating model (delivered risk).<br><br>It is important that the strength of the control environment is commensurate with: the risks involved; the sensitivity and criticality of the IT assets involved; and the level of trust that will be placed on the shared computing service environment. An understanding of the nature and strength of controls required is typically achieved through initial and periodic (or on material change) assessments of design and operating effectiveness (including alignment with industry agreed practices).<br><br>System administrator capabilities enable the execution of high impact activities and potentially provide unauthorized access to sensitive IT assets. Consequently, system administrator access entitlements would normally be subject to stronger controls, commensurate with the heightened risks involved. | Enabling customers to protect the confidentiality, integrity, and availability of systems and content is of the utmost importance to AWS, as is maintaining customer trust and confidence. To this end, AWS has established a formal audit program to validate the implementation and effectiveness of the AWS control environment.<br><br>The AWS audit program includes internal audits and third party accreditation audits. The objectives of these audits are to evaluate the operating effectiveness of the AWS control environment. Internal audits are planned and performed periodically. Audits by third party accreditation are conducted to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities.<br><br>Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications. Some key AWS audit programs and certifications are described under the heading "Assurance Program". For a full list of audits, certifications and attestations, see the AWS Assurance Programs webpage.<br><br>Regarding the control environment, AWS gives customers ownership and control over their customer content by design through simple, but powerful tools that allow customers to determine where their customer content will be stored, secure their customer content in transit or at rest, and manage access to AWS services and resources for their users. AWS implements technical and physical controls designed to prevent unauthorized access to or disclosure of customer content.<br><br>AWS seeks to maintain data integrity through all phases including transmission, storage, and processing. AWS treats all Customer data and associated assets as Highly Confidential. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. AWS is vigilant about customers' security and have implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure. |

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| | | Customer provided data is validated for integrity, and corrupted or tampered data is not written to storage. Amazon Simple Storage Service (S3) utilizes checksums internally to confirm the continued integrity of data in transit within the system and at rest. Amazon S3 provides a facility for customers to send checksums along with data transmitted to the service. The service validates the checksum upon receipt of the data to determine that no corruption occurred in transit. Regardless of whether a checksum is sent with an object to Amazon S3, the service utilizes checksums internally to confirm the continued integrity of data in transit within the system and at rest. When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy. External access to data stored in Amazon S3 is logged and the logs are retained for at least 90 days, including relevant access request information, such as the data accessor IP address, object, and operation.<br><br>Additional information on AWS security credentials can be found on the AWS Documentation website including information on understanding and getting security credentials. |
| **Ongoing management of material service providers** | Receiving sufficient information on a regular basis to enable effective oversight. This typically includes formal notification arrangements as part of change and incident management processes. | Regarding the AWS change management process, AWS service teams maintain service specific change management standards that inherit and build on the AWS Change Management guidelines.<br><br>AWS applies a systematic approach to managing change to ensure that changes to a production environment are reviewed, tested, and approved. The AWS Change Management approach requires that the following steps be completed before a change is deployed to the production environment:<br><br>1. Document and communicate the change via the appropriate AWS change management tool.<br>2. Plan implementation of the change and rollback procedures to minimize disruption.<br>3. Test the change in a logically segregated, non-production environment.<br>4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review.<br>5. Attain approval for the change by an authorized individual.<br><br>Where appropriate, a continuous deployment methodology is conducted to ensure changes are automatically built, tested, and pushed to production, with the goal of eliminating as many manual steps as possible. Continuous deployment seeks to eliminate the manual nature of this process and automate each step, allowing service teams to standardize the process and increase the efficiency with which they deploy code. In continuous deployment, an entire release process is a "pipeline" containing "stages".<br><br>AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. Firewall policies (configuration files) are automatically pushed to firewall devices every 24 hours. |

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| | | In order to validate that changes follow the standard change management procedures, all changes to the AWS production environment are reviewed on at least a monthly basis. An audit trail of the changes is maintained for a least a year.<br><br>Regarding the AWS incident management process, AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.<br><br>AWS utilizes a three-phased approach to manage incidents:<br><br>1. **Activation and Notification Phase** - Incidents for AWS begin with the detection of an event. Events originate from several sources such as:<br>• Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact customers<br>• Trouble tickets entered by an AWS employee.<br>• Calls to the 24x7x365 technical support hotline<br>• If the event meets incident criteria, the relevant on-call support engineer use Event Management Tool system to start an engagement and page relevant program resolvers (for example, Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.<br>2. **Recovery Phase** - The relevant resolvers will perform break fix to address the incident. After addressing troubleshooting, break fix and affected components, the call leader will assign follow-up documentation and follow-up actions and end the call engagement.<br>3. **Reconstitution Phase** - The call leader will declare the recovery phase complete after the relevant fix activities have been addressed. The post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and actions, such as design changes, will be captured in a Correction of Errors (COE) document and tracked to completion.<br><br>To ensure the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the AWS Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities. |

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| | | The Incident Response Test Plan is executed annually, in conjunction with the Incident Response plan. The test plan includes multiple scenarios, potential vectors of attack, the inclusion of the systems integrator in reporting and coordination (when applicable), as well as varying reporting/detection avenues (i.e. customer reporting/detecting, AWS reporting/detecting).<br><br>AWS Incident Management planning, testing and test results are reviewed by third party auditors.<br><br>Service teams will generate audit records in accordance with AWS audit policy, and may be directed to adjust their auditable events by service teams and security personnel supporting the service-specific functions. Changes to auditing requirements will be pushed out to the service teams for implementation via an internal tracking system, with an appropriate severity assigned, based upon the urgency of the threat situation, which will determine the time threshold required for the change. |
| **Business Disruption** | The ability to recover from a business disruption event is an important consideration when using shared computing services.<br><br>The following are important considerations as part of effective recovery capability when using shared computing services:<br><br>• Clarity regarding roles and responsibilities of the shared computing service provider, the ARI and other parties in the event of a disruption event (including crisis management, recovery initiation, coordination of recovery activities and communication)<br><br>• Clarity regarding the state to which the shared computing service will be recovered and the impact this has on recovery and backup activities of the ARI and other parties. This includes consideration of data, software and software configuration<br><br>• Ensuring that the security control environment of the alternate site meets production requirements | The AWs infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.<br><br>AWS provides customers with the flexibility to place instances and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.<br><br>Additionally, the AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been designed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach helps AWS perform system recovery and reconstitution efforts in a methodical sequence, aiming to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.<br><br>AWS maintains a ubiquitous security control environment across all Regions. Each data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+1 redundancy model to ensure system availability in the event of component failure. Components (N) have at least one independent backup component (+1), so the backup component is active in the operation even if all other components are fully functional. In order to eliminate single points of failure, this model is applied throughout AWS, including network and data center implementation. All data centers are online and serving traffic; no data center is "cold." In case of failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites. |

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| | • Ensuring that recovery strategies, when using shared computing services, are not exposed to the risk of the same event impacting production and recovery environments (e.g. use of out of band data backups, platform and physical segregation)<br>• A testing regime that verifies that recovery plans and strategies, when using share computing services, are effective and ensure business requirements (including recovery objectives relating to time, point, capacity and performance) are met in the event of a loss of availability | Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. Each Availability Zone is designed as an independent failure zone. In the case of failure, automated processes move customer data traffic away from the affected area. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains.<br>Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures, from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. |
| **Assurance** | An ARI normally seek regular assurance that risk and control frameworks, and their application, are designed and operating effectively in order to manage the risks associated with the use of a shared computing service.<br>The use of shared computing services may expose critical and/or sensitive IT assets to environments where an ARI is unable to enforce its IT security policy, such as public networks and shared infrastructure (i.e. 'un-trusted'). To mitigate this, an ARI could develop a schedule of assurance testing that ensures that all aspects of the IT security control environment, both of the ARI and the service provider, are assessed over time.<br>It is important that all of the dimensions in the auditable universe are assessed over time, commensurate with the risks involved, including (but not limited to) assessment of the following:<br>• Legal, regulatory and contractual compliance | Enabling customers to protect the confidentiality, integrity, and availability of systems and content is of the utmost importance to AWS, as is maintaining customer trust and confidence. To this end, AWS has established a formal audit program to validate the implementation and effectiveness of the AWS control environment.<br>Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001 and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.<br>Compliance reports from these assessments are made available to customers to enable them to evaluate AWS. The AWS Compliance reports identify the scope of AWS services and Regions assessed, as well the assessor's attestation of compliance. A vendor or supplier evaluation can be performed by leveraging these reports and certifications.<br>Some key AWS audit programs and certifications are described under the heading "Assurance Program". For a full list of audits, certifications and attestations, see the AWS Assurance Programs webpage.<br>Additionally, AWS formally tracks and monitors its regulatory and contractual agreements and obligations. In order to do so, AWS has performed and maintains the following activities:<br>• Identified applicable laws and regulations for each of the jurisdictions in which AWS operates<br>• Documented and maintains all statutory, regulatory and contractual requirements relevant to AWS |

| Area for Consideration | Information Paper Guidance (Non-Exhaustive) | AWS Controls |
|---|---|---|
| | • Management and oversight of the arrangement, including reporting mechanisms<br>• IT asset lifecycle management processes including: change, process scheduling, capacity, performance, incidents, access, software development and maintenance, backups, and logging<br>• Security management include: roles/responsibilities, security solutions deployed, vulnerability and patch management, incident detection and response; encryption key management and the boundaries isolating the ARI from other parties.<br>Business continuity and disaster recovery management, including backup testing arrangements for: data, software and software configuration | • Categorized records into types with details of retention periods and type of storage media via the Data Classification Policy<br>• Informed and trains personnel (e.g. employees, contractors, third party users) that must be made aware of compliance policies to protect sensitive AWS information (e.g. intellectual property rights and AWS records) via the Data Handling Policy<br>• Monitors the use of AWS facilities for unauthorized activities with a process in place to enforce appropriate disciplinary action<br>AWS maintains relationships with outside parties to monitor business and regulatory requirements. Should a new security directives issued, AWS has documented plans in place to implement that directive with designated time frames.<br>Refer to the following AWS Audit Reports for additional details: SOC 1, SOC 2, PCI DSS, ISO 27001, ISO 27017 |

# Next Steps

Each organization's cloud adoption journey is unique. In order to successfully execute your adoption you need to understand your organization's current state, the target state, and the transition required to achieve the target state. Knowing this will help you set goals and create work streams that will enable staff to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best-practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organization, throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find more about such workshops, please contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology at https://aws.amazon.com/professional-services/CAF/.

For ARIs in Australia, next steps typically also include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us at https://aws.amazon.com/contact-us/.
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the AWS Artifact portal (accessible via the AWS Management Console).
- Obtain and review a copy of the AWS APRA 234 Workbook from the AWS Artifact portal.
- Consider the relevance and application of the CIS AWS Foundations Benchmark available here and here, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this whitepaper and in the "Further Reading" section below.
- Speak to your AWS representative about an AWS Enterprise Agreement, and the introductory guide designed to help ARIs assess the AWS Enterprise Agreement against CPS 231.

# Further Reading

For additional help, see the following sources:

- AWS Best Practices for DDoS Resiliency
- AWS Security Checklist
- Securing Data at Rest with Encryption
- AWS Best Practices for DDoS Resiliency
- Cloud Adoption Framework - Security Perspective
- Introduction to AWS Security Processes
- AWS Security Best Practices
- Encrypting Data at Rest
- AWS Risk & Compliance
- Using AWS in the Context of Common Privacy and Data Protection Considerations
- Security at Scale: Logging in AWS
- Security at Scale: Governance in AWS
- Secure Content Delivery with CloudFront

# Document Revisions

| Date | Description |
| --- | --- |
| April 2018 | Migrated to new template. |
| December 2017 | First publication. |