AWS User Guide to Financial Services Regulations and Guidelines in Australia

October 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers, or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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

About this guide

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 (AWS) Cloud services.

Overview

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 through their use of cloud services. From July 2019, ARIs also need to comply with Prudential Standard CPS 234 on Information Security, which requires ARIs to maintain an information security capability commensurate with information security vulnerabilities and threats. ARIs who have a third party managing their information assets have until the earlier of the next contract renewal period with that third party or July 1, 2020, to comply with CPS 234.

While the use of Amazon Web Services (AWS) Cloud services by ARIs substantially pre-dates the release of the updated CPS 231 and CPS 234, AWS welcomes the increased clarity and guidance provided by APRA.

The following sections provide considerations for ARIs as they assess their responsibilities with regard 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.
- **CPS 234 Information Security** – This Prudential Standard states APRA's requirements relating to information security.
- **CPG 234 Information Security** – This Prudential practice guide provides APRA's guidance to ARIs on safeguarding IT assets.

- **APRA information paper on Outsourcing Involving Cloud Computing Services** – This information 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.

APRA's Prudential Standard CPS 230 Operational Risk Management

On July 17, 2023, APRA published the new Prudential Standard CPS 230 Operational Risk Management (CPS 230) aimed at ensuring that ARIs better manage operational risks and respond to business disruptions. CPS 230 will be effective from July 1, 2025, and will replace five existing standards, including CPS 231 and Prudential Standard CPS 232 Business Continuity.

At the time of publication of this guide, APRA is publicly seeking submissions on its draft Prudential Practice Guide CPG 230 Operational Risk Management (CPG 230), which will accompany CPS 230. AWS will author an update to this guide after the CPG 230 guidance is finalized.

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, applications, systems, and networks, no differently than they would for applications in an on-premises data center.

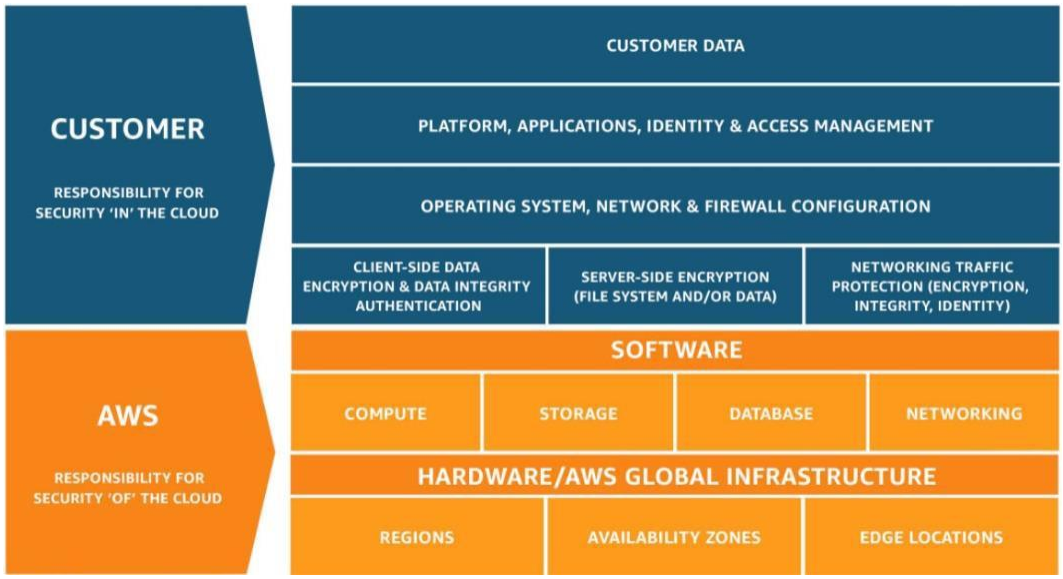

Figure 1: Shared Responsibility Model

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. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data.

Security in the cloud

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

It's 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 and AWS Region where they store their content.
- The format and structure of their content and whether it's 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. Customer responsibility is determined by the AWS services that a customer selects. This selection, in turn, determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as infrastructure as a service (IaaS) and, as such, requires the customer to perform all the necessary security configuration and management tasks. Customers that deploy an EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

For abstracted services, such as Amazon S3 and DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using AWS Identity and Access Management (IAM) tools to apply the appropriate permissions.

Security of the cloud

AWS infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use 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's 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 customers can implement, 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 applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS compliance 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 that follow 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 ISO 27001 Compliance.

- **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 implementation guidance for information security controls that's specific to cloud service providers. For more information or to download the AWS ISO 27017 certification, see ISO 27017 Compliance.
- **ISO 27018** – ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It's based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls that's 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 that aren't addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see ISO 27018 Compliance.
- **ISO 9001** – ISO 9001 outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures that are required to achieve effective quality management within an organisation. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organisational 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 ISO 9001 Compliance.
- **PCI DSS Level 1** – The Payment Card Industry Data Security Standard (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) 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 PCI DSS Compliance.

- **SOC** – AWS System and Organisation 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 that have been established to support operations and compliance. For more information, see SOC Compliance. There are five types of AWS SOC Reports:
    - **SOC 1:** Provides information about the AWS control environment that might be relevant to a customer's internal controls over financial reporting, as well as information for assessment of the effectiveness of internal controls over financial reporting.
    - **SOC 2:** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
    - **SOC 2 (Amazon DocumentDB):** Provides customers and their service users who have a business need with an independent assessment of the AWS control environment relevant to Amazon DocumentDB system security, availability, and confidentiality.
    - **SOC 2 Privacy Type I Report:** Provides customers with an independent assessment of AWS systems and the suitability of the design of AWS privacy controls.
    - **SOC 3:** Provides customers and their service users who have 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 Compliance Programs webpage. For information about general AWS security controls and service-specific security, see Best Practices for Security, Identity, and Compliance.

AWS Artifact

Customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS Global Infrastructure

The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location around the world where we cluster data centers. We call each group of logical data centers an Availability Zone (AZ). Each Region consists of multiple isolated and physically separate AZs within a geographic area. Each AZ has independent power, cooling, and physical security and is connected by redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZs to achieve even greater fault-tolerance. Customers can learn more about these topics by downloading the Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond whitepaper.

AWS customers choose the Regions in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud. For example, AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) Region or the AWS Asia Pacific (Melbourne) 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 and AWS Asia Pacific (Melbourne) Region are designed and built to meet rigorous compliance standards globally, providing high levels of security for AWS customers. As with every Region, the Asia Pacific (Sydney) Region and AWS Asia Pacific (Melbourne) Region are compliant with applicable national and global data protection laws.

AWS customers choose the Regions 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 AWS customers. As with every 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 has the potential, if disrupted, to have a significant impact on the ARI's business operations 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's 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 CPS 231 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 after 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	AWS considers this an action for the ARI to independently complete.

Due diligence requirement	Customer considerations
for selecting the service provider	

Due diligence requirement	Customer considerations
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. The financial statements of Amazon.com, Inc. include AWS sales and income, permitting assessment of its financial position and ability to service its debts and liabilities. These financial statements are available from the SEC or at the Amazon Investor Relations website. The Amazon.com, Inc. Form 10-K filing is available at the Amazon 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. 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. 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.

Due diligence requirement	Customer considerations
	See the following AWS Audit Reports for additional details: SOC 2, PCI DSS, ISO 27001, and ISO 27017. Amazon.com, Inc. has a Code of Business Conduct and Ethics, available at the Amazon Investor Relations website that 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 enroll 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.

Due diligence requirement	Customer considerations
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 Compliance Programs webpage. Compliance reports from these assessments are made available through 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. 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.

Due diligence requirement	Customer considerations
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 Cloud Storage on AWS. Additionally, AWS offers AWS Database Migration Service (AWS DMS), a web service customers can use to migrate a database from an AWS service to an on-premises database.

Outsourcing agreement

Paragraph 28 of CPS 231 requires each ARI to 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 enroll 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 upon entering into 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.

CPS 234 – Information security

CPS 234 outlines the measures ARIs should take to be resilient against information security incidents (including cyber-attacks). CPS 234 defines an *information security incident* as an actual or potential compromise of information security.

CPS 234 requires ARIs to maintain an information security capability commensurate with information security vulnerabilities and threats. A key objective is to minimize the likelihood and impact of information security incidents on the confidentiality, integrity, or availability of information assets, including information assets managed by related parties or third parties. Key requirements of CPS 234 include that an ARI must:

- Clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies, and individuals.
- Maintain an information security capability commensurate with the size and extent of threats to its information assets, which enables the continued sound operation of the ARI.
- Implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets and undertake systematic testing and assurance regarding the effectiveness of those controls.
- Notify APRA of material information security incidents.

A full analysis of CPS 234 is beyond the scope of this document. However, the following sections address the considerations in CPS 234 that most frequently arise in interactions with ARIs.

Roles and responsibilities

Paragraphs 13 and 14 of CPS 234 state that the Board of an ARI must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and that enables the continued sound operation of the ARI. Additionally, ARIs must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies, and individuals with responsibility for decision-making, approval, oversight, operations, and other information security functions.

While AWS considers the ARI's definition of information security-related roles and responsibilities as an action for the ARI to independently complete, there are a number of AWS resources and services available to help customers meet these requirements.

A common theme among the most successful customers of AWS is that they have an engaged board and senior management team who are enthusiastic about the benefits of moving to the cloud and are aware of the changed risks and responsibilities of operating in the cloud. The AWS C-suite Guide to Shared Responsibility for Cloud Security and Data Safe Cloud eBook on the AWS Data Safe Cloud Checklist site inform boards and senior management about the benefits and risks of operating in the cloud.

At an operational level, IAM enables customers to manage access to AWS services and resources securely. Using IAM, customers can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM can be used to grant employees and applications federated access to the AWS Management Console and AWS service APIs, using existing identity systems such as Microsoft Active Directory or an identity management solution that supports Security Assertion Markup Language (SAML) 2.0.

IAM helps customers analyze access across their AWS environments. Security teams and administrators can quickly validate that policies only provide the intended public and cross-account access to resources, and customers can also identify and refine policies to allow access to only the services being used.

This helps customers to better adhere to the principle of least privilege—granting only the permissions required to perform a task.

Multi-factor authentication (MFA) for highly privileged users, using AWS multi-factor authentication, is a security feature that augments username and password credentials.

MFA requires users to prove physical possession of a hardware MFA token or MFA-enabled mobile device by providing a valid MFA code.

Information security capability

Paragraphs 15 to 17 of CPS 234 require ARIs to have an information security capability commensurate with the size and extent of threats to their information assets and to assess the information security capability of any related or third party who manages information assets of the ARI. An ARI is also required to actively maintain its information security capability with respect to changes in vulnerabilities and threats. CPS 234 defines an *information security capability* as the totality of resources, skills and controls that provide the ability and capacity to maintain information security.

AWS has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems and content. AWS maintains a broad range of industry and geography specific compliance programs and is continually assessed by external certifying bodies and independent auditors to provide assurance the policies, processes, and controls established and operated by AWS are in alignment with these program standards and the highest industry standards.

AWS considers the development and maintenance of an ARI's information security capability as an action for the ARI to independently complete. The following resources help customers meet these requirements.

A range of security, identify, and compliance whitepapers are available for download from AWS. AWS training and certification programs offer a range of free digital courses, classroom-based training, and AWS certifications to develop and maintain an information security capability to help meet APRA requirements.

AWS Managed Services (AMS) and AWS Security Competency Partners can be used by customers to augment internal capabilities or to fill gaps where recruiting in-house resources is cost-prohibitive or while in-house capability is being developed. AMS can automate common activities, such as change requests, monitoring, patch management, security, and backup services, and provides full lifecycle services to provision, run, and support customer infrastructure. AWS Security Competency Partners support customers in multiple areas including infrastructure security, policy management, identity management, security monitoring, vulnerability management, data protection, and consulting services.

Policy framework

Paragraphs 18 and 19 of CPS 234 require ARIs to maintain an information security policy framework commensurate with their exposures to vulnerabilities and threats. This policy must provide direction on the responsibilities to all parties who have an obligation to maintain information security.

AWS implements formal, documented policies and procedures that provide guidance for operations and information security within an AWS organization and the supporting AWS environments. Policies address purpose, scope, roles, responsibilities, and management commitment.

AWS considers the development and maintenance of an ARI's information security policy framework as an action for the ARI to independently complete. The following AWS services can assist with policy implementation and compliance monitoring to help customers meet their above-the-line compliance requirements with this area of CPS 234.

In conjunction with IAM policies, AWS customers can use AWS Organizations to implement service control policy (SCP) permission guardrails to ensure that users can only perform actions that meet corporate security and compliance policy requirements. Additionally, customers can configure central logging of actions performed across their organization using AWS CloudTrail and centrally aggregate data for AWS Config, enabling customers to audit their environment for compliance and react quickly to changes.

AWS Control Tower allows customers to set up and govern a secure, compliant, multi-account AWS environment based on best practices established by working with thousands of enterprises. With AWS Control Tower, users on distributed teams can provision new AWS accounts quickly. Meanwhile, central cloud administrators will know that all accounts are aligned with centrally established, company-wide compliance policies.

Information asset identification and classification

Paragraph 20 of CPS 234 requires ARIs to classify their information assets (software, hardware, and data) by criticality and sensitivity, including those managed by related parties and third parties. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect—

financially or non-financially—the entity or the interests of depositors, policyholders, beneficiaries, or other customers.

To ensure asset management inventory and maintenance procedures are properly implemented, AWS assets are assigned an owner, tracked, and monitored with AWS proprietary inventory management tools.

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 our customers' security and has 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's stored, used, and protected from disclosure.

AWS considers the identification and classification of an ARI's information assets an action for the ARI to independently complete. The following AWS services and resources might assist customers.

AWS Config provides a detailed inventory of customers' AWS resources and configuration, and continuously records configuration changes. Amazon CloudWatch provides data and actionable insights to monitor applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

AWS Systems Manager gives visibility and control of customer infrastructure on AWS. Systems Manager provides a unified user interface to view operational data from multiple AWS services and allows automation of operational tasks across AWS resources. AWS Systems Manager Inventory provides visibility into Amazon EC2 and on-premises computing environments by collecting metadata from your managed instances.

Customers can store metadata in a central Amazon S3 bucket, and then use built-in tools to query the data and quickly determine which instances are running the software and configurations required by policy, and which instances need to be updated. Customers can configure Inventory on all managed instances by using a one-click procedure and configure and view inventory data from multiple Regions and accounts.

AWS Cost Management tools give customers visibility into AWS costs and usage. There is a range of Cost Management tools to help access, organize, understand, control, and optimize costs, which is an important aspect of cloud governance.

Implementation of controls

Paragraphs 21 and 22 of CPS 234 require ARIs to ensure information security controls are in place to protect their information assets (software, hardware, and data), including those managed by related parties and third parties. These controls must be commensurate with vulnerabilities and threats to the information assets, criticality and sensitivity of the information assets, the lifecycle stage of the information asset, and the potential consequences of an information security incident.

AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within AWS organizations. AWS management reviews and evaluates the risks identified in the risk management program at least annually. The risk management program encompasses the following phases:

- Discovery – The discovery phase includes listing out risks (threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Research – The research phase considers the potential impacts of identified risks to the business and its likelihood of occurrence and includes an evaluation of internal control effectiveness.
- Evaluate – The evaluate phase includes ensuring controls, processes, and other physical and virtual safeguards in place to prevent and detect identified and assessed risks.
- Resolve – The resolve phase results in risk reports provided to managers with the data they need to make effective business decisions and to comply with internal policies and applicable regulations.
- Monitor – The monitor phase includes performing monitoring activities to evaluate whether processes, initiatives, functions, and activities are mitigating the risk as designed.

The implementation of controls to protect information assets is a shared responsibility between AWS and ARIs. The following AWS services and resources can assist customers with their portion of shared controls.

AWS Artifact provides on-demand access to AWS security and compliance reports, encompassing over 2,500 controls. Reports include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

AWS defines the most important aspects of security *in* the cloud for customers through mechanisms such as the AWS Well-Architected Framework and the AWS Cloud Adoption Framework. Both of those frameworks have specific security areas including detailed whitepapers that help focus on how to design and build secure cloud environments.

Incident management

Paragraphs 23 to 26 of CPS 234 require ARIs to have robust mechanisms in place to detect and respond timely to information security incidents, as well as respond to those incidents the ARI considers could plausibly occur (that is, information security response plans). An ARI's information security response plan must include the mechanisms for managing all relevant stages of an incident including escalation and reporting. ARIs must annually review and test their information security response plans to ensure they remain effective and fit-for-purpose.

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.

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 through detection and analysis, containment, eradication, recovery, and post-incident activities.

AWS runs its Incident Response Test Plan 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 and detection avenues (such as customer reporting and detecting and AWS reporting and detecting).

AWS considers the development and implementation of mechanisms and plans to detect and respond to information security incidents as a shared responsibility between AWS and ARIs. The effectiveness of AWS controls for its portion of these shared responsibilities is described in the assurance reports available in AWS Artifact.

For customer responsibilities, and as mentioned in the guidance in the Roles and Responsibilities section above, AWS Managed Services (AMS) and AWS Security Competency Partners can be used by customers to augment internal capabilities or to fill gaps where recruiting in-house resources is cost prohibitive. AWS Security Competency Partners support customers in multiple areas including infrastructure security, policy management, identity management, security monitoring, vulnerability management, data protection, and consulting services.

The AWS Security Incident Response Guide presents an overview of the fundamentals of responding to security incidents within a customer's AWS Cloud environment. It focuses on an overview of cloud security and incident response concepts, and identifies cloud capabilities, services, and mechanisms that are available to customers who are responding to security issues.

With CloudTrail, customers can discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account within a specified period of time. AWS Config allows customers to continuously audit and assess the overall compliance of AWS resource configurations with organizational policies and guidelines.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect customers' AWS accounts and workloads. Amazon Detective automatically collects log data from AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables faster and more efficient security investigations.

Finally, AWS Security Hub gives customers a comprehensive view of high-priority security alerts and compliance status across their AWS accounts. With Security Hub, customers have a single place that aggregates, organizes, and prioritizes security alerts, or findings, from multiple AWS services. Security Hub became generally available in June 2019 in many Regions around the world, including the AWS Asia Pacific (Sydney) Region.

Testing control effectiveness

Paragraphs 27 and 28 of CPS 234 require ARIs to test the effectiveness of their information security controls through a systematic testing program. The nature and frequency of this testing program must be commensurate with the rate at which the vulnerabilities and threats change, the criticality and sensitivity of the information assets, the consequences of information security incidents, the risks associated with exposure to environments where the ARI is unable to enforce its information security policies, and the materiality and frequency of change to information assets. Where an ARI's information assets are managed by a related party or third party and the ARI is reliant on that party's information security control testing, the ARI must assess whether the nature and frequency of testing of controls is commensurate with the above items.

Paragraphs 29 to 31 of CPS 234 require ARIs to escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner and to ensure that the testing is conducted by appropriately skilled and functionally independent specialists. ARIs must also review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment.

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.

AWS plans and performs internal and external audits according to a documented audit schedule to review the continued performance of AWS against standards-based criteria like the ISO/IEC 27001 and to identify improvement opportunities.

AWS plans and performs external audits according to a documented audit schedule to review the continued performance of AWS against standards-based criteria and to identify improvement opportunities. The AWS Compliance reports identify the scope of AWS services and regions assessed, as well the assessor's attestation of compliance.

AWS considers the testing of information security controls as a shared responsibility between AWS and ARIs. The effectiveness of AWS controls for its shared responsibilities is described in the assurance reports available in AWS Artifact.

To help customers meet CPS234 requirement for their portion of shared controls, Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector

automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports, which are available through the Amazon Inspector console or API.

Amazon Inspector security assessments also check for unintended network accessibility of Amazon EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered as pre-defined rules packages mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for access to your EC2 instances from the internet, remote root login being enabled, or vulnerable software versions installed. These rules are regularly updated by AWS security researchers.

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for eight services:

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Internal audit

Paragraphs 32 and 33 of CPS 234 require an ARI's internal audit activities to review the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance). ARIs must ensure that this information security control assurance is provided by appropriately skilled personnel.

Paragraph 34 of CPS 234 states that an ARI's internal audit function must assess the information security control assurance provided by a related party or third party where:

a. An information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.

b. The ARI's internal audit function intends to rely on the information security control assurance provided by the related party or third party.

AWS Compliance reports are made available to customers to enable them to evaluate AWS. AWS considers the audit of information security controls to validate the design and operating effectiveness as a shared responsibility between AWS and ARIs.

For customers auditing of their own environments, CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across their AWS infrastructure. CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

APRA notification

Paragraphs 35 and 36 of CPS 234 require ARIs to notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policy holders, beneficiaries, or other customers or that has been notified to other regulators. An ARI must also notify APRA as soon as possible and no later than 10 business days, after it becomes aware of a material information security control weakness that the entity expects it will not be able to remediate in a timely manner.

AWS defines, administers, and monitors for security incidents for the underlying cloud infrastructure. AWS will promptly notify a customer and take reasonable steps to reduce the effects of a security incident if AWS becomes aware of any unlawful or unauthorized access to customer data on AWS equipment or in AWS facilities, and if this unlawful or unauthorized access results in loss, disclosure, or alteration of customer data.

Depending on contract requirements, AWS maintains procedures for notifying customers of customer-impacting issues using the AWS Service Health Dashboard. The AWS Service Health Dashboard publishes up-to-the-minute information on service availability, where customers can subscribe to an RSS feed to be notified of

interruptions to each individual service and a full status history of each individual service health.

CPS 234 doesn't explicitly require contractual commitments from an outsourcing service provider beyond those already contained in APRA's pre-existing Prudential Standards CPS 231 (Outsourcing) and SPS 231 (Outsourcing). AWS customers that are APRA-regulated institutions have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs, including to address the regulatory compliance requirements of CPS 231 and SPS 231.

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

AWS gives customers access to the necessary information to help them meet APRA's notification requirements under CPS 234, paragraphs 35 and 36. There are three ways for customers to get notifications of the status of the workloads they have running on AWS. The best source of security and privacy events related to AWS services are the AWS Security Bulletins, which AWS uses to keep its customers apprised of security announcements, including the AWS timelines for remediation.

The AWS Service Health Dashboard publishes up-to-the-minute information on service availability in Regions around the world. Customers can also take advantage of near real time monitoring and alerting services such as CloudTrail, CloudWatch, GuardDuty, and Security Hub. Customers are always encouraged to implement any manner of auditing, intrusion detection, or other detective controls that monitor for attempted unauthorized access within the instances and services they are using in AWS.

Customers can integrate these sources into automatic notification platforms, for example by subscribing to the RSS feeds for the AWS Service Health Dashboard and the AWS Security Bulletins. Monitoring these sites is the best way for customers to access the information required to help meet APRA's requirements for notification.

Customers should also keep their accounts up to date with accurate email addresses and security contact information to facilitate timely response and notification.

CPG 234 – Management of security risk in information and information technology

CPG 234 Information Security (CPG 234) provides APRA's guidance on particular areas to assist ARIs in the management of information security. CPG 234 doesn't 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:

- Considerations for the Board
- Roles and responsibilities
- Information security capability
- Policy framework
- Information asset identification and classification
- Implementation of controls
- Incident management
- Testing control effectiveness
- Internal audit
- Notification

CPG 234 also provides additional specific guidance in the form of the following attachments:

- Security principles
- Training and awareness
- Identity and access
- Software security
- Cryptographic techniques

- Customer security
- Testing techniques
- Reporting

AWS has produced an AWS CPG 234 Workbook that documents relevant controls and guidance (referencing the AWS Well-Architected Framework) for each of the CPG 234 guidelines. The Workbook covers the 10 sections and 8 attachments 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 is a sample of the AWS response to CPG 234's *Implementation of controls* section:

Guideline	Responsibility	Response
54-55:	AWS	Data security and privacy – Key generation
Cryptographic techniques to restrict access	AWS control objective	AWS establishes and manages cryptographic keys for required cryptography employed within the system boundary. AWS produces, controls, and distributes symmetric cryptographic keys using U.S. National Institute of Standards and Technology (NIST)-approved key management technology and processes in the AWS information system. An AWS-developed secure key and credential manager is used to create, protect, and distribute symmetric keys, and is used to secure and distribute: • AWS credentials needed on hosts • RSA public/private keys • X.509 Certificates Cryptographic keys are securely stored and periodically rotated.
54-55:	Customer	Well-Architected – Question and Best Practice: SEC-9 – How do you protect your data at rest? • Implement secure key management Encryption keys must be stored securely and rotated with strict access control, for example, by using a key management service such as AWS Key Management Service (AWS KMS). Consider using different keys for segregation of different data classification levels and retention requirements.
Cryptographic techniques to restrict access	Well-Architected Framework	

ARIs can obtain a copy of the AWS CPG 234 Workbook through 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.

Information paper on outsourcing involving cloud computing services

Published in September 2018, APRA's information paper on "Outsourcing Involving Cloud Computing Services" highlights recommendations and key principles that APRA states should be considered by an ARI when it contemplates using cloud computing services. The information paper excludes arrangements where IT assets are dedicated to a single ARI such as private cloud arrangements.

APRA states in the introduction of the information paper that cloud computing service providers have strengthened their control environments, increased transparency regarding the nature of the controls in place, and improved their customers' ability to monitor their environments since the previous information paper was published in 2015.

APRA considers that systems of records (SoR) maintain information essential to determining obligations to customers and counterparties, such as current balance, benefits, and transaction history. Arrangements involving SoR are classified as extreme inherent risk by APRA, and it's expected that ARIs can demonstrate that their risk management and mitigation techniques and capabilities are sufficiently strong. Refer to the *APRA notification and consultation* section later in this guide for commentary on the notification and consultation steps APRA encourages for arrangements involving extreme inherent risk.

This section of the guide focuses on Chapters 2 (Risk management considerations) and 3 (APRA notification and consultation) of the information paper.

Risk management considerations

Chapter 2 of the information paper outlines a non-exhaustive list of other considerations for assessment by ARIs when using cloud computing services. This section includes introductory information relevant to those considerations.

Selection process

Information paper guidance (non-exhaustive): A comprehensive due diligence process, including independent assessments, rather than placing sole reliance on attestations by the service provider and customer references, would normally be conducted. The intent would typically be to verify the maturity, adequacy, and appropriateness of the provider and services selected (including the associated control environment), taking into account the intended use of the cloud computing service.

Post solution design, ARIs should conduct a risk assessment to consider:

- The ability for the ARI to avoid a significant impact on business operations and meet obligations regardless of technology, people, process, or service provider failure.
- The ability to meet performance, capacity, security, high-availability, recoverability, and other business requirements.
- The adequacy of secure design principles and development practices.
- The adequacy of processes to verify that software operates as intended within the cloud computing service.
- The critical and sensitive IT assets that are accessible from the shared computing service.
- The ability to meet legislative and prudential requirements (including the outsourcing standards).
- Any impediments that could inhibit APRA's ability to fulfil its duties as a prudential regulator.

AWS controls: 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.

The financial statements of Amazon.com, Inc. include AWS sales and income, permitting assessment of its financial position and ability to service its debts and liabilities. These financial statements are available from the SEC or at the Amazon Investor Relations website.

A list of customer references and corresponding case studies can be found on the AWS Customer Success website.

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.

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.

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 can add redundant systems, backups, locations, network uplinks, and so on, to create a more resilient, high availability architecture. If a customer requires restricted access, AWS enables customers to implement access rights management controls both on a systems level and through encryption on a data level.

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.

AWS customers have the option to enroll in an Enterprise Agreement with AWS to tailor agreements that best suit their needs. AWS also provides an introductory guide to help ARIs assess the AWS Enterprise Agreement against the applicable regulatory requirements.

Risk assessments and security

Information paper guidance (non-exhaustive): An ARI would normally conduct initial and periodic security and risk assessments of all material service provision arrangements. Security and risk assessments would typically be conducted whenever a material change to existing arrangements occurs.

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.
- The criticality and sensitivity of the IT assets involved.
- The transition process.
- The target operating model.

It's important that the strength of the control environment is commensurate with:

- The risks involved.
- The sensitivity and criticality of the IT assets involved.
- The level of trust that will be placed on the cloud computing service environment.
- The shared responsibilities between the service provider and entity.

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.

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.

AWS controls: 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.

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.

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 has 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's stored, used, and protected from disclosure.

Customer provided data is validated for integrity, and corrupted or tampered data is not written to storage. Amazon S3 uses 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 uses 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.

Additional information on AWS security credentials can be found on the AWS Documentation website, including information on understanding and obtaining security credentials.

Implementation of controls

Information paper guidance (non-exhaustive): The nature of cloud computing services necessitates the allocation of responsibility for the implementation of controls between the provider and the client. It would be prudent for ARIs to carefully consider the differing levels of responsibility for operating and managing these arrangements.

An ARI would normally have the capability to evaluate the design and operating effectiveness of controls within the shared responsibility model, with a level of assessment commensurate with the impact on the ARI if the service is compromised.

This normally involves evaluations initiated by the ARI as well as the use of audit reports initiated by the service provider, conducted by an independent third party. It's important that the ARI considers the adequacy of audit reports initiated by the service provider for this purpose and supplement the reports when considered deficient.

An important control objective is the timely detection of unauthorized access and use of the ARI's environment by the service provider's staff, service accounts, other customers, or third parties. This includes any changes to the environment that might weaken preventative controls. An ARI would normally have controls for responding in a timely manner to these alerts.

AWS controls: AWS employs a shared responsibility model for data ownership and security. AWS operates, manages, and controls the infrastructure components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

AWS services in production operations are managed in a manner that preserves their confidentiality, integrity, and availability. AWS has implemented secure software development procedures that are followed to ensure appropriate security controls are incorporated into the application design.

As part of the application design process, new applications must participate in an AWS Security review including registering the application, initiating the application risk classification, participating in the architecture review and threat modeling, performing code review, and performing a penetration test.

Customers assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewalls and other security, change management, and logging features.

AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their Amazon instances and applications.

For more information, see the *Security and shared responsibility* and *AWS compliance programs* sections of this guide.

Ongoing oversight

Information paper guidance (non-exhaustive): 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.

AWS controls: 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.

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:

1. Document and communicate the change using the appropriate AWS change management tool.
2. Plan implementation of the change and rollback procedures to minimize disruption.
3. Test the change in a logically segregated, non-production environment.
4. Complete a peer-review of the change with a focus on business impact and technical rigor. The review should include a code review.
5. Attain approval for the change by an authorized individual.

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*.

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.

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 at least a year.

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.

AWS uses a three-phased approach to manage incidents:

Activation and notification phase – Incidents for AWS begin with the detection of an event. Events originate from several sources such as:

- Metrics and alarms. AWS maintains an exceptional situational awareness capability, most issues are rapidly detected through 24/7/365 monitoring and alarming of real time metrics and service dashboards. Most incidents are detected in this manner. AWS uses early indicator alarms to proactively identify issues that might ultimately impact customers.
- Trouble tickets entered by an AWS employee.
- Calls to the 24/7/365 technical support hotline.

If an event meets incident criteria, the relevant on-call support engineer uses the event management tool to start an engagement and page relevant program resolvers (for example, the 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.

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.

Reconstitution phase – The call leader will declare the recovery phase complete after the relevant fix activities have been addressed.

The postmortem and deep root-cause analysis of the incident will be assigned to the relevant team. The results of the postmortem 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.

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.

AWS runs its Incident Response Test Plan 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 and detection avenues (customer reporting and detecting and AWS reporting and detecting).

AWS incident management planning, testing, and test results are reviewed by third-party auditors. Service teams will generate audit records in accordance with AWS audit policy and might 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 through 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

Information paper guidance (non-exhaustive): APRA expects that an ARI would continue to meet its obligations regardless of disruptions resulting from a failure of technology, people, process, or service providers. The following are important considerations as part of effective recovery capability when using shared computing services:

- Clarity regarding roles and responsibilities of the cloud computing service provider, the ARI, and other parties in the event of a disruption event (including crisis management, recovery initiation, co-ordination of recovery activities, and communication).

- Clarity regarding the state to which the cloud 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 software and data hosted on the service and configuration settings.
- Ensuring that the security control environment of the recovery solution meets production requirements.
- Ensuring that recovery strategies aren't exposed to the risk of the same event impacting production and recovery environments (for example, the use of out-of-band data backups and platform and physical segregation).
- A testing regime that verifies that recovery plans and strategies 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.

AWS controls: 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.

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 by different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

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.

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 use 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. 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.

Customers use 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.

Audit and assurance

Information paper guidance (non-exhaustive): An ARI would normally provide assurance to the Board that material service provision arrangements are appropriately managed, and that the service provision management framework is effective.

The assurance model normally involves a combination of internal audits (resourced internally and by independent expertise) as well as the use of audit reports initiated by the service provider, conducted by an independent third party.

One of the challenges for obtaining an adequate level of assurance over cloud computing services is balancing the needs of multiple customers with the practicalities of not overburdening the service provider. This could be addressed through a collaborative assurance model where assurance work is designed to meet the needs of the various customers.

It's important that all the dimensions in the auditable universe are assessed over time, commensurate with the risks involved, including (but not limited to) assessment of the following:

- Legal, regulatory, and contractual compliance.
- Management and oversight of the arrangement, including reporting mechanisms.
- IT asset lifecycle management processes including change, process scheduling, capacity, performance, incidents, access, software development and maintenance, backups, and logging.

- Security management including roles and responsibilities, security solutions deployed, vulnerability and patch management, incident detection and response, encryption key management, and the boundaries isolating the ARI from other parties.
- Business continuity and disaster recovery management, including backup testing arrangements for data, software, and software configuration.

AWS controls: 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.

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 include but are not limited to the ISO/IEC 27001 and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.

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.

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 using these reports and certifications.

Some key AWS audit programs and certifications are described in the *AWS compliance programs* section of this guide. For a full list of audits, certifications, and attestations, see the AWS Compliance Programs webpage.

Additionally, AWS formally tracks and monitors its regulatory and contractual agreements and obligations. To do so, AWS has performed and maintains the following activities:

- Identified applicable laws and regulations for each of the jurisdictions in which AWS operates.
- AWS documents and maintains statutory, regulatory, and contractual requirements relevant to AWS.
- Categorized records into types with details of retention periods and type of storage media through the Data Classification Policy.
- Informed and trains personnel (employees, contractors, and third-party users) that must be made aware of compliance policies to protect sensitive AWS information (intellectual property rights and AWS records) through the Data Handling Policy.
- Monitors the use of AWS facilities for unauthorized activities with a process in place to enforce appropriate disciplinary action.
- AWS maintains relationships with outside parties to monitor business and regulatory requirements. Should a new security directive be issued, AWS has documented plans in place to implement that directive with designated time frames.

See the following AWS Audit Reports for additional details: SOC 1, SOC 2, PCI DSS, ISO 27001, and ISO 27017.

APRA notification and consultation

When using cloud computing services, APRA states it's 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 and a range of other disruption scenarios.
- Preservation of the quality (including security) of both critical and sensitive data.
- Compliance with legislative and prudential requirements.
- Absence of jurisdictional, contractual, or technical considerations that might inhibit APRA's ability to fulfil its duties as prudential regulator, including impediments to timely access to documentation and data or information.

CPS 231 requires ARIs to consult with APRA prior to entering into an outsourcing arrangement that involves a material business activity where offshoring is involved. Additionally, in the information paper, APRA encourages ARIs to consult with APRA when the proposed outsourcing arrangement involves the use of cloud computing services and involves *heightened inherent risks* or *extreme inherent risks*, regardless of whether offshoring is involved.

APRA believes that environments that are available to non-financial industry entities (such as public cloud) should be treated as if they have such heightened inherent risks. For initiatives with *heightened inherent risk*, APRA states that consultation would typically take place after the ARI has completed its internal governance processes, and the initiative has been fully risk-assessed and approved by the appropriate governance authority. APRA also encourages early consultation for uses involving *extreme inherent risks* to provide APRA with the ability to give feedback on areas of potential concern prior to the ARI committing large amounts of resources to the initiative.

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

- Overview of the solution selected and rationale, due diligence, IT assets in scope, services and products selected, parties involved, and delivery locations.
- The ARIs materiality assessment, including impact on business processes, systems architecture, organization, and operating model.
- Risk and control assessments.
- Disaster recovery strategy.
- Contingency plans for provider failure.
- Evidence of approval by the appropriate governance authority.

To facilitate the consultation process, ARIs could also provide the documentation used to inform their internal governance mechanisms. APRA also recognizes that, given the need to consult early in situations of *extreme inherent risk*, not all of the above documentation will be available or completed at the start of the assessment.

Next steps

Each organization's cloud adoption journey is unique. To successfully complete your adoption, you must 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 learn more about such workshops, contact your AWS representative. Alternatively, AWS provides access to tools and resources for self- service application of the AWS CAF methodology at AWS Cloud Adoption Framework.

For ARIs in Australia, next steps typically also include:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solutions Architects, Professional Services teams, and Training instructors can assist with your cloud adoption journey. Contact us if you don't have an AWS representative.
- Obtain and review a copy of the latest AWS SOC 1 and 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification, from the AWS Artifact portal (accessible through 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 at CIS Amazon Web Services Foundations and CIS Amazon Web Services Three-tier Web, 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 guide and in the *Additional resources* section that follows.

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.

Contributors

Contributors to this document include:

- Katherine Velos, Corporate Counsel, Amazon Web Services
- Julian Busic, Security Architect, Amazon Web Services
- Krish De, Principal Solutions Architect (Governance, Risk and Compliance), Amazon Web Services
- Paul Curtis, Compliance Specialist, Amazon Web Services
- Clayton Ford, Public Policy Senior Manager, Amazon Web Services

Additional resources

For additional information, see:

- Financial Services Industry Lens – AWS Well-Architected Framework
- Using AWS in the Context of Australian Privacy Considerations
- AWS Best Practices for DDoS Resiliency
- AWS Security Checklist
- Cloud Adoption Framework – Security Perspective
- AWS Security Best Practices
- AWS Risk and Compliance

Document revisions

Date	Description
October 2023	Updates to reflect AWS Melbourne Region and CPS230
July 2020	Updates to APRA CPS 234 section to include guidance to customers on how AWS helps them with above-the-line compliance.
July 2019	Updated for APRA Prudential Practice Guide CPG 234 “Information Security” published on 25 June 2019.
December 2018	Updated for APRA Prudential Standard CPS 234 “Information Security” published on 13 November 2018.
October 2018	Updated for APRA Information Paper “Outsourcing involving cloud computing services” published on 24 September 2018.
December 2017	First publication.