AWS User Guide to Financial Services Regulations and Guidelines in Australia

July 2025

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 (APRA) as they accelerate their use of Amazon Web Services (AWS) Cloud services.

Overview

Background

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).

Introduction of Prudential Standard CPS 230 Operational Risk Management

On July 17, 2023, APRA published the Prudential Standard CPS 230 Operational Risk Management (CPS 230) aimed at ensuring that ARIs effectively manage their operational risks, maintain critical operations through disruptions, and manage the risks arising from service providers. In effect from July 1, 2025, CPS 230 replaces five existing standards,[i] including Prudential Standard CPS 231 Outsourcing (CPS 231) and Prudential Standard CPS 232 Business Continuity (CPS 232).

On February 19, 2025, APRA rescinded its 2018 Information Paper "Outsourcing Involving Cloud Computing Services". Instead, APRA expects all regulated entities to comply with CPS 230 requirements when using cloud services to appropriately manage associated risks and maintain operational resilience.

The introduction of CPS 230 has not impacted ARIs' need to comply with Prudential Standard CPS 234 on Information Security (CPS 234), which requires ARIs to maintain information security capabilities commensurate with information security vulnerabilities and threats.

About this user guide

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

- **Prudential Standard CPS 230 Operational Risk Management (CPS 230)** – this Prudential Standard states APRA's requirements relating to operational risk.
- **Prudential Practice Guide CPG 230 Operational Risk Management (CPG 230)** – this Prudential practice guide provides APRA's guidance relating to operational risk management.
- **Prudential Standard CPS 234 Information Security (CPS 234)** – this Prudential Standard states APRA's requirements relating to information security.

- **Prudential Practice Guide CPG 234 Information Security (CPG 234)** – this Prudential practice guide provides APRA's guidance to ARIs on safeguarding IT assets.

Taken together, ARIs can use this information for their due diligence and implementation of an appropriate information security, risk management, and governance program for their use of AWS.

Operational resilience, AWS and the Shared Responsibility Model

AWS and the financial services industry share a common interest in maintaining operational resilience capabilities; for example, the ability to provide continuous service despite disruptions. Continuity of services, especially for critical functions, is a key prerequisite for financial stability. AWS recognizes that financial institutions that use AWS need to comply with sector-specific regulatory obligations and internal requirements regarding operational resilience, such as CPS 230.

At AWS, we define operational resilience as the ability to provide continuous service through people, processes, and technology that are aware of and adaptable to constant change. It is a real-time, execution-oriented norm embedded in the culture of AWS that is distinct from traditional approaches in information security, business continuity, disaster recovery, and crisis management, which rely primarily on centralized, hierarchical programs focused on documentation development and maintenance.

However, operational resilience is a shared responsibility; AWS is responsible for making sure that the services used by our customers - the building blocks for their applications - are continuously available and making sure that we are prepared to handle a wide range of events that could affect our cloud infrastructure. AWS customers are responsible for designing, testing, and deploying their applications on AWS in a manner that achieves the availability and resiliency they need, including those mission-critical applications that require that AWS services are available when customers need them, even upon the occurrence of a service impairment and/or disruption.

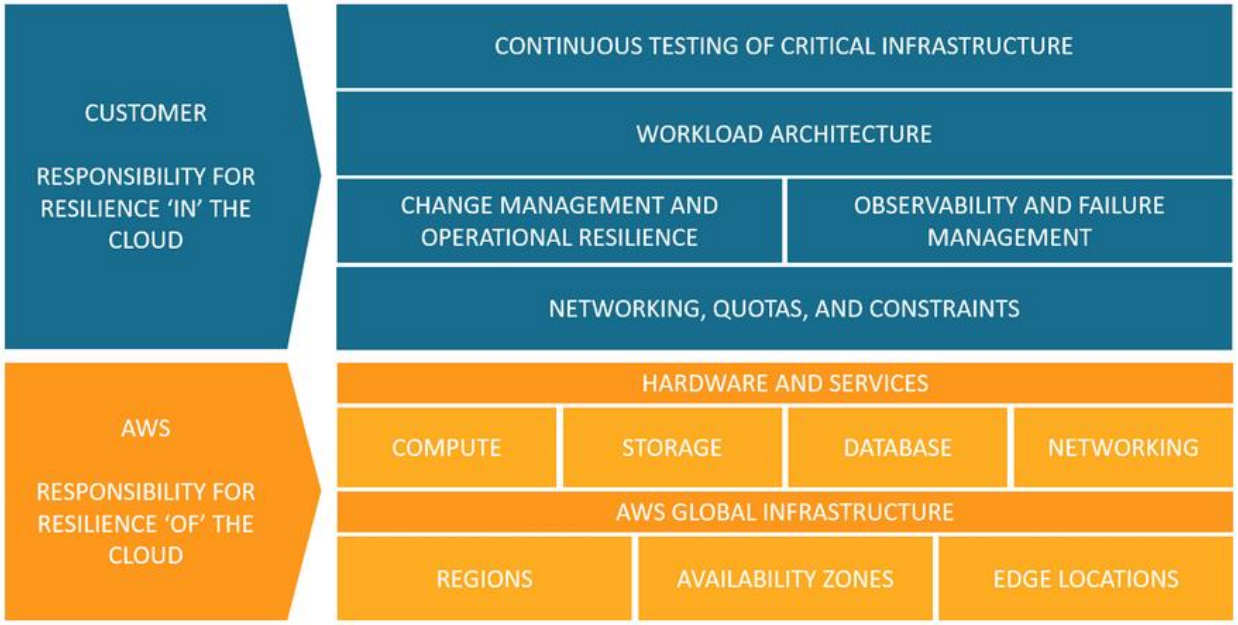

Figure 1: AWS Shared Responsibility Model for Operational Resilience

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of AWS and its customers within the context of cloud services. AWS is responsible for the resiliency of the hardware, software, networking, and facilities that run the services offered by AWS.

The responsibility of AWS customers is determined by the AWS services they select, because the service selection determines the amount of configuration work that customers must perform as part of their resiliency responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) requires customers to perform all the necessary resiliency configuration and management tasks. Customers that deploy Amazon EC2 instances are responsible for deploying Amazon EC2 instances across multiple locations (such as AWS Availability Zones), and can implement self-healing architectures using services such as Amazon EC2 Auto Scaling, and using resilient workload architecture best practices for applications installed on the Amazon EC2 instances.

For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and environments, and customers access the endpoints to store and retrieve data. Customers are responsible for managing resiliency of their data, including backup,

versioning and replication strategies, classifying their assets, and using identity and access management tools to apply the appropriate permissions.

Resilience of the cloud

AWS infrastructure and services operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of internal controls at AWS, including security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validating** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement, and to better assist customers with managing their control environment.
- **Demonstrating** the AWS compliance posture to help customers assess 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 that have been established and operated by AWS. ARIs can use this information to perform their control evaluation and verification procedures.
- **Monitoring** through security controls that AWS remains aligned with global standards and best practices.

Resilience in the cloud

AWS customers are responsible for their resilience in the cloud and assume the responsibility and management of the guest operating system (including updates and security patches) and other associated application software, in addition to applicable network security controls. Customers should carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

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

AWS provides tools and information to assist customers assessing controls in their extended IT environment. For more information, see the AWS Compliance Center, Amazon Web Services' Approach to Operational Resilience in the Financial Sector and Beyond, Shared Responsibility Model for Resiliency, and the AWS Well Architected Framework. Contact your AWS representative to discuss how the AWS FSI Compliance team, the AWS Partner Network, as well as AWS Solution Architects, and Professional Services teams can assist.

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 are applicable to storing personally identifiable information (PII) in public cloud services. 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 27701** – Specifies requirements and guidelines to establish and continuously improve a Privacy Information Management System (PIMS), including processing of PII. It is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management and provides a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processors and controllers not addressed by the existing ISO/IEC 27002 control set. For more information or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.
- **ISO 22301** – Specifies the structure and requirements to implement, maintain, and improve a business continuity management system (BCMS) to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise. Compliance with this standard underscore the business continuity and resiliency of AWS services. For more information or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.

- **ISO 42001** – ISO/IEC 42001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. It is designed for entities providing or using AI-based products or services, facilitating responsible development and use of AI systems. For more information or to download the AWS ISO 42001 certification, see the ISO 42001 Compliance webpage
- **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 organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information or to download the AWS ISO 9001 certification, see 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 AWS PCI DSS Attestation of Compliance and Responsibility Summary, see PCI DSS Compliance.
- **SOC** – AWS System and Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls 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, in addition to 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 builds 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.

Support plans

Customers can take advantage of AWS Support plans that are designed to give customers the right mix of tools and access to expertise so that customers can be

successful with AWS while optimizing performance, managing risk, and keeping costs under control.

Basic Support is included for AWS customers and includes:

- Customer Service and Communities offer 24/7 access to customer service, documentation, whitepapers, and AWS re:Post.
- AWS Trusted Advisor is designed to provide seven core Trusted Advisor checks and guidance to provision resources following best practices to increase performance and improve security.
- AWS Health is designed to provide a personalized view of the health of AWS services, and alerts when customer resources are impacted.

AWS Enterprise Support is recommended for customers planning to operate critical operations on AWS. AWS Enterprise Support assists customers to manage, monitor, analyze, and report on usage of AWS. AWS Enterprise Support provides customers with proactive planning, architectural reviews, and consultative guidance including strategic business reviews, security improvement programs, guided Well-Architected reviews, and cost optimization workshops. AWS Enterprise Support also includes:

- A designated Technical Account Manager (TAM) to provide consultative architectural and operational guidance delivered in the context of your applications and use-cases to help you achieve the greatest value from AWS.
- A response time within 15 minutes in the case of a business-critical system going down.
- Consultative reviews and guidance based on your applications.
- Access to proactive reviews, workshops, and deep dives.
- Full set of checks and prioritized recommendations curated by your AWS account team with AWS Trusted Advisor Priority.
- 24/7 phone, web, and chat access to Cloud Support Engineers.

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 aligned with applicable national and global data protection laws.

CPS 230 – Operational Risk Management

On July 17, 2023, APRA published CPS 230 to ensure that ARIs are resilient to operational risks and disruptions. CPS 230 requires regulated financial entities to effectively manage their operational risks, maintain critical operations during disruptions, and manage the risks associated with service providers. In effect from July 1, 2025, CPS 230 replaces five existing standards, including CPS 231 Outsourcing and CPS 232 Business Continuity. Note that ARIs that already have pre-existing agreements with material services providers do not need to update these agreements in accordance with CPS 230 until July 1, 2026.

AWS published the AWS Workbook for the APRA CPS 230 to support AWS customers as they work to meet applicable CPS 230 requirements. The workbook describes

operational resilience, AWS and the Shared Responsibility Model, AWS compliance programs, and relevant AWS services and whitepapers that relate to regulatory requirements. The workbook is complementary to this document and is available through AWS Artifact.

To assist in meeting the CPS 230 requirements we recommend referring to APRA's CPG 230 and the compliance checklist outlined in APRA's Response to submissions - CPG 230 Operational Risk Management.

CPS 234 – Information Security

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

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.

AWS published the AWS Workbook for the APRA CPG 234 available through AWS Artifact to support AWS customers as they work to meet applicable CPS 234 requirements and CPG 234 observations. The workbook is intended as a reference and supporting document to assist ARIs in their own preparation for a compliance review with APRA. Where applicable, under the AWS shared responsibility model, the

workbook provides supporting AWS details and references to assist ARIs when adapting CPG 234 for their workloads on AWS.

To assist in meeting the CPS 234 requirements and CPG 234 observations, we recommend referring to APRA's CPG 234, APRA's August 2024 letter on Additional insights on common cyber resilience weaknesses and APRA's June 2024 letter on Security and adequacy of backups.

See Appendix 1 for a summary of key aspects for CPS 234 and CPG 234.

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 aims to break 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, AWS 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 AWS Artifact (accessible through the AWS Management Console).

- Obtain and review a copy of the AWS Workbook for CPS230 Operational Risk Management from AWS Artifact.
- Obtain and review a copy of the APRA CPG 234 Workbook from AWS Artifact.

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 into other governance and risk management practices as necessary based on your due diligence and risk assessment, using the tools and resources referenced throughout this document and in the *Additional resources* section that follows.

Contributors

Contributors to this document include:

- Katherine Velos, Legal, 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

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
- AWS User Guide to Governance, Risk and Compliance for Responsible AI Adoption within Financial Services Industries

Document revisions

Date	Description
July 2025	Addition of CPS 230 and recognition of the rescinding of the APRA Information Paper “Outsourcing involving cloud computing services”
October 2023	Updates to reflect AWS Melbourne Region and CPS 230
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.

Appendix 1: Key aspects of APRA CPS234

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, customers can use AWS Identity and Access Management (IAM) 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.

Using AWS multi-factor authentication (MFA) is an IAM best practice that requires a second authentication factor in addition to user name and password sign-in 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 complimentary 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 help make sure 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.

Customers can use AWS Control Tower to set up and govern a secure, compliance-aligned, 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 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 help make sure that 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 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 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 have 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 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 making sure controls, processes, and other physical and virtual safeguards are in place to help 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, and to 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 help verify 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 threats, the inclusion of the systems integrator in reporting and coordination (when applicable), in addition to 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 Information security capability 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 help 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.

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.

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 CPS 234 requirements 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.

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, and

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 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.

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.

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 manners 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 systems, 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.

Appendix 2: Key aspects of CPG 234

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, help 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: **Cryptographic techniques to restrict access**	Customer Well-Architected Framework	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.

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.

---

[i] Prudential Standard CPS 231 Outsourcing (CPS 231), Prudential Standard SPS 231 Outsourcing (SPS 231), Prudential Standard HPS 231 Outsourcing (HPS 231), Prudential Standard CPS 232 Business Continuity Management (CPS 232) and Prudential Standard SPS 232 Business Continuity Management (SPS 232).