Guide to Financial Services Regulations in Chile

Financial Markets Commission (CMF) RAN 20-7

November 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.

Additionally, this document does not constitute legal advice and should not be relied on as legal advice. AWS encourages its customers to obtain appropriate advice on their implementation of privacy and data protection environments, and more generally, applicable laws relevant to their business.

Contents

Abstract

Financial services institutions in Chile classified as banks and regulated by the Financial Markets Commission (Comisión para el Mercado Financiero or CMF) need to comply with the Recopilación Actualizada de Normas 20-7 (RAN 20-7) as they adopt the Amazon Web Services (AWS) Cloud. RAN 20-7 includes specific contractual, operational, and technical requirements for financial institutions when outsourcing Information Technology (IT) services to cloud service providers.

This guide describes the roles that AWS and customers play in managing and securing the cloud environment, describes the AWS Shared Responsibility Model, and provides an overview of the regulatory requirements and guidance from the CMF that regulated financial institutions can consider when adopting AWS.

Introduction

The Comisión para el Mercado Financiero (CMF) is Chile's primary regulatory agency in charge of regulating and overseeing the use of cloud services by financial institutions. The CMF possesses regulatory authority over a broad set of financial institutions in Chile, including banks, their affiliates and supporting companies, payment card issuers and operators, and loans and savings cooperatives, among others. The specific regulatory requirements applicable to financial institutions, including those related to the outsourcing of technology services, vary depending on the classification of the financial institutions and the applicable regulatory authority and regulation. This guide is relevant to financial institutions classified as banks in Chile.

The CMF issued the Recopilación Actualizada de Normas 20-7 (RAN 20-7) in 2019 to compile the rules applicable to financial institutions regulated by the CMF. RAN 20-7 includes specific contractual, operational, and technical requirements with which regulated financial institutions must comply when outsourcing Information Technology (IT) services to cloud service providers.

This guide is a resource to help financial institutions in Chile understand the technical and operational requirements that might apply to them under RAN 20-7 when they use AWS. This document also describes the AWS compliance framework and advanced tools and security measures that financial institutions might find helpful when evaluating and demonstrating their compliance with the applicable regulatory requirements under RAN 20-7.

A full analysis of RAN 20-7 is beyond the scope of this guide. However, the following sections address the primary considerations that occur in our interactions with financial institutions in Chile and provide information that institutions can use to help them understand their responsibilities under RAN 20-7.

- **Security and shared responsibility:** financial institutions understand the AWS Shared Responsibility Model before evaluating the specific technical and operational requirements outlined in RAN 20-7. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS with respect to security and information access.

- **AWS compliance programs:** AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can use the AWS compliance programs to help satisfy their regulatory requirements.
- **AWS Global cloud infrastructure:** The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones (AZs). The AWS Global Cloud Infrastructure offers AWS customers a more effective way to design and operate applications and databases, making them more available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to help them design an AWS environment consistent with their business and regulatory needs, including applicable requirements under RAN 20-7.
- **Considerations on RAN 20-7:** This section sets out common considerations for financial institutions that use AWS as they consider some of the key technical and operational requirements under RAN 20-7 and describes how financial institutions can use AWS services and tools to help them comply with their regulatory requirements. A list of requirements and corresponding considerations is provided in the Appendix, AWS Considerations on Operational and Security Requirements under RAN 20-7 Regulation.

This document is provided for informational purposes only; it is not legal or compliance advice and should not be relied on as legal or compliance advice. Customers are responsible for making their own independent assessments and should obtain appropriate advice from their own legal and compliance advisors regarding compliance with applicable regulations.

Security and the AWS Shared Responsibility Model

Cloud security is a shared responsibility and financial institutions need to understand the AWS Shared Responsibility Model before reviewing their operational and technical requirements under RAN 20-7. AWS manages security of the cloud by maintaining the AWS Cloud Infrastructure aligned with global and regional regulatory requirements and best practices. Security in the cloud is the responsibility of the customer. Namely, our customers retain control of the security programs that they choose to implement to protect their content, applications, systems, and networks, because they are responsible for applications in an on-premises data center.

Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud.

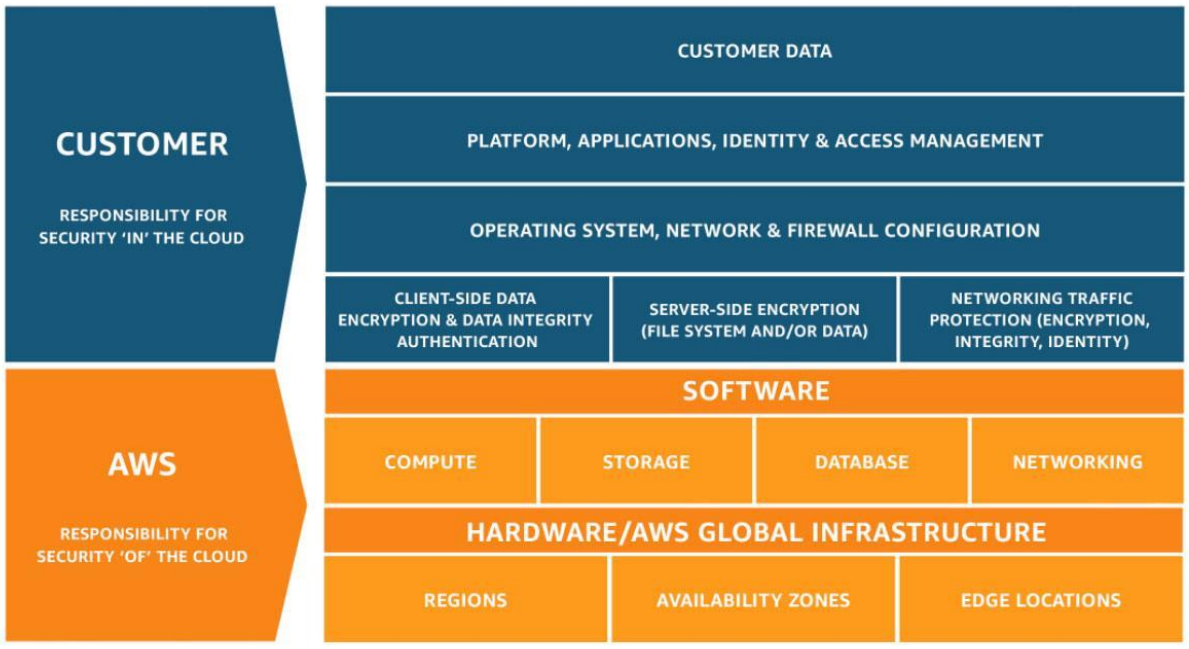

Figure 1 – The AWS Shared Responsibility Model

AWS responsibility “Security of the Cloud” – AWS is responsible for protecting the infrastructure that runs the services offered in the AWS Cloud. This infrastructure is

composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility "Security in the Cloud" – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This 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 of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including installing updates and security patches) and other associated application software, as well as applicable network security controls.

For abstracted services, such as 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 their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

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 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; and
- Who has access to their content, and how those access rights are granted, managed, and revoked.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated

with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer.

AWS Compliance programs

AWS has obtained certifications and independent third-party attestations for a variety of industry-specific workloads. The following compliance programs can be of particular importance to financial institutions:

- **ISO 27001** – 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 the ISO 27001 Compliance webpage.
- **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 specific to cloud service providers. For more information or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.
- **ISO 27018** – Code of practice that focuses on protecting personal data in the cloud. It is based on the ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls that is applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

- **ISO 9001** – 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 the ISO 9001 Compliance webpage.
- **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. Amazon Web Services (AWS) is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. For more information or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.
- **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 the SOC Compliance webpage. AWS SOC Reports come in three forms:
    - **SOC 1**: Provides information about the AWS control environment that may be relevant to a customer's internal controls over financial reporting, as well as information for the assessment of the effectiveness of internal controls over financial reporting.
    - **SOC 2**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
    - **SOC 3**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality, without disclosing AWS internal information.

See the AWS Compliance Programs webpage for more information about AWS certifications and attestations. See the Best Practices for Security, Identity, & Compliance website for general AWS security controls and service-specific security.

AWS Artifact

Customers can use AWS Artifact to review and download reports and details about more than 2,600 security controls. In addition, 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

The AWS Support plans 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 all AWS customers and includes:

- Customer Service & Communities – 24x7 access to customer service, documentation, whitepapers, and support forums.
- AWS Trusted Advisor – Access to the seven core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.
- AWS Personal Health Dashboard – A personalized view of the health of AWS services, and alerts when your resources are impacted.

AWS Global Cloud infrastructure

The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones. A Region is a physical location in the world that consist of multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These Availability Zones offer customers the ability to operate applications and databases, which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment. Customers can learn more about these topics by downloading our whitepaper on Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

AWS customers choose the AWS Region(s) where their content and applications are located. AWS Regions allow customers to establish environments that meet specific geographic or regulatory requirements. Additionally, AWS Regions allow 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.

Considerations on Recopilación Actualizada de Normas de Bancos (RAN)

Financial institutions are mainly governed by the Recopilación Actualizada de Normas de Bancos (also known as RAN) issued by the CMF. The focus of this guide is RAN Chapter 20-7 (RAN 20-7), which regulates the outsourcing of services by financial institutions, including cloud services. However, we note that other chapters of RAN regulate the use of cloud services by financial institutions, including among others, RAN Chapter 20-8 (RAN 20-8) and RAN Chapter 20-9 (RAN 20-9) also mentioned in this guide.

RAN Chapter 20-7: Outsourcing of services

The CMF allows financial institutions to outsource IT services to third-party cloud services providers operating in Chile or abroad. RAN 20-7 does not require financial institutions to obtain a formal approval from the CMF prior to contracting cloud service providers nor does it require financial institutions to notify such contracting to the CMF. RAN 20-7 imposes specific requirements on financial institutions that decide to outsource IT services to cloud service providers that operate outside of Chile, including, but not limited to:

- Maintaining certain records about the service provider, including for example, records that support the financial reliability of the service provider and that show that it maintains certifications demonstrating the quality and safety of its services, and the existence of systems controls.
- For some financial institutions, maintaining a contingency data processing center located in Chile. For more information, see the business continuity section later in this document.

Regulatory supervision, audit, and inspection

Financial institutions must verify that the CMF has permanent access either through visits conducted at the cloud service provider facilities or remotely to all records, data, and information being processed, held, and generated through an external provider whether established in the country or abroad. For more information, refer to Externalizacion de Servicios.

Financial institutions can enroll in an AWS Enterprise Agreement that gives them the option to tailor agreements that best suit their needs, including regulatory requirements. Through an AWS Enterprise Agreement, AWS offers its financial institution customers regulated by the CMF a contractual framework that helps them satisfy applicable contractual requirements under the RAN 20-7, including specific terms that address the access and inspection rights of the regulator, where required by applicable law and under certain conditions. For more information about AWS Enterprise Agreements, contact your AWS representative.

Data localization

RAN 20-7 provides that when financial institutions outsource services, data, technological services, and applications to be used in the outsourced services must be found on specific processing sites, and in the cases of foreign processing; such data, technological services and applications must be in a defined and known jurisdiction. The parties must also know the city in which the data centers are located. For more information, refer to Externalizacion de Servicios, Capítulo 20-7.

With AWS, customers own their customer data and control its location. AWS gives its customers the option to choose between several AWS Regions where their content and servers are located. In addition, through our PCI-DSS Level 1 certification available on AWS Artifact, the automated compliance-reporting portal, customers will know the exact city within each AWS Regions where data centers are located.

Additionally, financial institutions that need to analyze data latency and residency requirements can consider using AWS Local Zones or AWS Outposts. AWS Local Zones are a type of AWS infrastructure deployment that places compute, storage, database, and other selected services closer to large populations, industries, and IT centers. AWS Outposts is a pool of fully managed solutions delivering AWS infrastructure and services to on-premises or edge locations for a consistent hybrid experience; helping customers to extend and run native AWS services on premises. Both types of infrastructure enable customers to deliver applications that require single-digit millisecond latency to end users and, under certain scenarios, require compliance with data localization requirements.

Technical and operational requirements

Security incidents

Financial institutions must report to the CMF operational incidents that affect or jeopardize their business continuity, the funds of the financial institutions or its customers, the quality of services, or the public image of the financial institutions. Such incidents include, but are not limited to, failure in the services provided by critical providers, or technological problems that affect the security of information. Financial institutions must notify CMF of these incidents within thirty (30) minutes after their occurrence and must maintain a permanent communication channel, as defined in RAN 20-8. For more information, refer to Información de Incidentes Operacionales.

AWS has implemented a formal, documented incident response policy and program to respond to potential security threats in accordance with the AWS Shared Responsibility Model. AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods. Auditing occurs on the systems and devices, and information is then aggregated and stored in a proprietary tool for review and incident investigation. All remote administrative access attempts are logged and limited to a specific number of attempts. Auditing logs are reviewed by the AWS Security team for unauthorized attempts or suspicious activity. When suspicious activity is detected, the incident response procedures are initiated. This information can be reviewed in SOC 2 Report, which is available to customers under a non-disclosure agreement. For more information, see the AWS Artifact section earlier in this document.

Under the AWS Shared Responsibility Model, AWS customers are responsible for establishing and documenting usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access allowed to their systems (including multi-factor authentication) in accordance with their access control policy. AWS customers are responsible for authorizing remote access to their systems prior to allowing such connections. Regulated financial institutions can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub, and AWS Config Rules to track, monitor, analyze, and audit events.

AWS also maintains public notification security bulletins, available in the AWS Security Center. For more information about how AWS maintains consistently high levels of security, refer to Best Practices for Security, Identity, & Compliance.

Business continuity

Obligations, guidelines, operational and technical requirements for financial institutions regarding business continuity management are primarily found in RAN 20-7 and RAN 20-9. The main business continuity management obligations applicable to financial institutions are:

- General management elements.
- Data processing sites and technological infrastructure.
- Systemic contingencies.

For more information, see: Gestión de la continuidad del negocio, Capítulo 20-9.

The Business Continuity Plan (BCP) details the process that AWS follows in the case of an outage, from detection to deactivation. This plan has been developed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach helps verify that AWS performs system recovery and reconstitution efforts in a methodical sequence, maximizing the effectiveness of the recovery and reconstitution efforts and minimizing system outage time due to errors and omissions.

AWS maintains a ubiquitous security control environment across all AWS Regions. Financial institutions and other 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. Financial institutions can learn more about how to architect disaster recovery in the AWS Cloud with the AWS Elastic Disaster Recovery (AWS DRS).

RAN 20-7 provides that financial institutions that outsource the processing of “significant or strategic” workloads abroad must maintain a contingency Data Processing Center located in Chile and demonstrate a recovery time compatible with the criticality of the outsourced service. Therefore, financial institutions must determine if the workloads they outsource are considered “significant or strategic.” RAN 20-7 does not consider cloud services “significant or strategic” *per se*, but provides examples of activities it considers to be “significant or strategic” such as these:

- Activities of such importance that any weakness or failure in the provision or management of the service has a significant effect on regulatory compliance, business continuity, information security (either the financial institution's information or the customers') and the quality of services, products, information, and the contracting financial institution's image and reputation.
- Any activity that involves the processing of data that is subject to banking confidentiality or secrecy according to the provisions of the General Banking Law.
- Any activity having a significant impact on risk management.
- Activities with high systematic interaction in the environment or that incorporate significant risks for the contracting financial institutions.

For more information, refer to Externalización de servicios.

Exceptionally, under specific circumstances, financial institutions that maintain adequate operational risk management, as determined by the CMF in its latest evaluation of the corresponding financial institutions following RAN 1-13, might waive this requirement as long as they comply with certain requirements as detailed in Servicios realizados en el extranjero (section IV. 1 b). For more information, see the Appendix to this guide.

Getting started

Each organization's cloud adoption journey is unique; and so, you need to understand your organization's current state, the desired target state, and the transition required to achieve the target state to manage your cloud adoption successfully. Knowing this helps you set goals and create work streams that enables staff to thrive in the cloud.

For financial institutions in Chile, the next steps typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from AWS Artifact that is accessible through the AWS Management Console.

- Consider the relevance and application of the AWS security whitepapers, AWS Well-Architected Framework, and the CIS Amazon Web Services Foundations Benchmark, as appropriate for your cloud journey and use cases. These industry-accepted best practices, provide AWS customers with clear, step-by-step implementation and assessment recommendations.
- Explore other governance and risk management practices as necessary, do due diligence and risk assessment, using the tools and resources referenced throughout this guide.
- Contact your AWS representative to obtain additional information regarding the AWS Enterprise Agreement and determine the support level that matches your needs.

In addition to helping our customers maximize the use of the technology provided by AWS, the AWS technical team can support our customers in their efforts to implement architecture, products, and services in compliance with applicable technical and operational requirements under RAN 20-7.

Further reading

The following resources can help financial institutions think about security and compliance when designing a secure and resilient environment on AWS.

- AWS Security & Compliance Quick Reference Guide AWS has many features to assist you in aligning with compliance objectives for your regulated workloads in the AWS Cloud. These features can help you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, simpler operations, and improved agility by providing more oversight, security control, and central automation.
- AWS Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS best practices. The recommendations are built around a single-page architecture that includes AWS security services—how they help achieve security objectives, where they can be best deployed and managed in your AWS accounts, and how they interact with other security services. This overall architectural guidance complements detailed, service-specific recommendations such as those found on AWS Security Documentation.

- The AWS Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help you implement designs that scale application needs over time. The AWS Well-Architected Framework consists of six pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- AWS whitepapers on the six pillars of the AWS Well-Architected Framework: Operational Excellence Pillar; Security Pillar; Reliability Pillar; Performance Efficiency Pillar; Cost Optimization Pillar, and the Sustainability Pillar.
- Global Financial Services Regulatory Principles: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS Cloud services and specifically, applying the Shared Responsibility Model to their regulatory requirements. You can review these principles on AWS Artifact.
- NIST Cybersecurity Framework (CSF): The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (that is, security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS Cloud offerings conformance to NIST CSF risk management practices (that is, security of the cloud). Financial institutions can use NIST CSF and AWS resources to elevate their risk management frameworks.

For more information, refer to the Security Learning whitepapers.

Appendix: AWS considerations on operational and security requirements under RAN 20-7 regulation

The following sections list key technical and operational requirements identified in RAN 20-7 along with AWS considerations to assist financial institution customers in understanding each requirement when using AWS, and a description of the best practices from the AWS Well-Architected Framework, which financial institutions can use to support their compliance efforts.

The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability —the Well-Architected Framework provides a consistent approach for customers to evaluate architectures and implement designs that scale over time.

The table is organized into the following columns:

- **Requirements:** Lists the requirements in RAN 20-7.
- **AWS Considerations:** Explains the considerations for addressing the requirements identified in RAN 20-7. It refers to security and compliance of the cloud, how AWS implements and manages controls, and AWS services that financial institution customers can use to address requirements in the Regulation.
- **Implementation:** Lists best practices for security in the cloud from the AWS Well-Architected Framework that financial institutions can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services is available in the AWS Well-Architected Framework.

III. CONDITIONS THAT MUST BE MET IN THE OUTSOURCING OF SERVICES

The entity that decides to outsource any activity, in addition to considering the aspects indicated in Annex No. 1 for the purposes of contracting each particular service, must comply with the following conditions:

1. General conditions

Requirements	AWS Considerations	Implementation
a) The Board of Directors must decide on the risk tolerance that it is willing to assume in the case of outsourcing services.	**Customer responsibility.** AWS customers are responsible for defining their operational process model for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.
b) Maintain a policy duly approved by the Board of Directors, which regulates the activities associated with outsourcing. This policy must pronounce itself, at least, on the elements indicated in No. 2 as follows.	**Customer responsibility.** AWS Customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.
c) Verify that the provider has mechanisms in place to prevent actions taken by other customers from negatively affecting the service outsourced by the entity.	**Shared responsibility.** AWS 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. Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualized operational environments to customers (that is, Amazon Elastic Compute Cloud (Amazon EC2)) checks that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure through hypervisors and instance isolation.	Not applicable.

Requirements	AWS Considerations	Implementation
	Different instances running on the same physical machine are isolated from each other through the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. Packets must pass through this layer; thus, an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms. Customer instances have no access to physical disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data using traditional filesystem encryption mechanisms or, in the case of Amazon Elastic Block Store (Amazon EBS) volumes, by enabling AWS-managed disk encryption. Customers can learn more about Logical Separation on the Logical Separation on AWS whitepaper and Infrastructure Security user guide.	
d) Establish formal procedures for the selection, contracting and monitoring of suppliers.	**Customer responsibility.** AWS Customers are responsible for defining their governance, risk assessment, and operational model. AWS Customers can use these AWS services to monitor performance. 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.	Not applicable.

Requirements	AWS Considerations	Implementation
	Amazon CloudWatch is a monitoring service for AWS Cloud resources and the workloads that run on AWS. AWS Customers can use CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. CloudWatch can monitor AWS resources such as EC2 instances and Amazon Relational Database Service (Amazon RDS) DB instances, as well as custom metrics generated by customers' workloads and services, and any log files your applications generate. Customers can use CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react and keep your workload running smoothly. Customers can learn more about this topic in: Monitoring, AWS User Engagement Service Level Agreement, AWS Service Level Agreements (SLAs).	
e) Check that the supplier and the staff in charge of the contracted services possess adequate knowledge and experience. Likewise, it must also monitor the due compliance with those regulatory and legal aspects that could affect the provision of the contracted services (such as labor laws).	**Shared responsibility.** AWS Customers are responsible for defining their own internal Training and Awareness program. AWS Customers can use AWS training services and resources to check their staff have the appropriate training and resources to manage AWS services. Training offerings can be found at Training and Certification. AWS has implemented formal, documented security awareness, and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes. The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties. AWS has developed, documented and disseminated role-based security awareness training for employees responsible for designing, developing, implementing, operating, maintaining, and monitoring the systems managing security and availability and provides resources necessary for employees to fulfill their responsibilities.	Not applicable.

Requirements	AWS Considerations	Implementation
f) Maintain an updated inventory of all services contracted with external companies, clearly determining those that, in their opinion, are strategic and high risk, in order to establish control and monitoring procedures permanently according to the levels of criticality assigned to them.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.
g) Establish procedures that verify timely and full compliance with the commitments it has with its customers.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.
h) Verify that there are independent audits of the selection, contracting, and monitoring process of suppliers, with personnel specialized in the different risks audited.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.
i) Verify that the provider periodically carries out internal audit reports or independent reviews of its services, in accordance with its structure and the size of its organization, and must share in a timely manner with the institution the findings that are pertinent to it. **j)** Require service providers that the operational, administrative and technological procedures of the contracted service be duly documented, updated and permanently available for review by this Superintendence.	**Shared responsibility.** AWS Customers can use AWS Artifact, the automated compliance reporting portal available in the AWS Management Console, 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 Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.	Not applicable.

Requirements	AWS Considerations	Implementation
	There are four AWS SOC Reports available to AWS customers from AWS Artifact: ○ AWS SOC 1 Report. ○ AWS SOC 2 Security, Availability & Confidentiality Report. ○ AWS SOC 2 Privacy Type I Report. ○ AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper. AWS internal and external audits are planned and performed according to the documented audit schedule to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.	
k) Consider the risks that come from the outsourced service chains, which must be reflected in the respective contract in advance, noting that in case of subcontracting, the subcontracted company must also comply with the conditions agreed between the entity and the initial service provider. Likewise, the responsibilities and obligations that the subcontracted companies must fulfill with respect to the service outsourced by the entity must be clearly established in the respective contracts.	**Shared responsibility.** AWS financial institution customers have the option to enroll in an Enterprise Agreement with AWS. Through an AWS Enterprise Agreement, AWS offers financial institutions regulated by the CMF a contractual framework that might help them satisfy the applicable contractual requirements under the RAN 20-7, including requirements in relation to the use of subcontractors. For more information about AWS Enterprise Agreements, please contact your AWS representative.	Not applicable.

Requirements	AWS Considerations	Implementation
l) The entity must incorporate in the operational risk reports for the Board of Directors, or for whoever takes its place, information regarding the actions carried out by the institution to manage outsourcing risks, including changes in the risk profile of suppliers (for example, relevant changes in their processes and geographical areas from where the services are provided), and exposure to those services considered critical.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use. AWS keeps our data center locations strictly confidential to maintain the security and privacy of customer data. The naming convention for our AWS Regions is indicative of the general geographic location of the Availability Zones and data centers that make-up that AWS Region. Additional detail regarding the general location of data centers is contained in our PCI-DSS report available through AWS Artifact. To learn more, see our AWS Global Infrastructure web page.	Not applicable.
m) The data, technological services and applications to be used in the outsourcing of services must be located in specific processing sites and in the case of processing abroad, in a defined and known jurisdiction. In addition to the jurisdiction, you should know the city where the data centers operate.	**Customer responsibility.** The AWS customer can choose the AWS Region or Regions in which their content is located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. AWS services are structured so that a customer maintains effective control of customer content regardless of what AWS Region they use for their content. This allows customers to establish environments that meet specific geographic or regulatory requirements. Customers can replicate and back up their content in more than one AWS Region. AWS won't move or replicate customers' content outside of their chosen AWS Region(s) without their agreement, except as necessary to comply with the law. AWS keeps our data center locations strictly confidential to maintain the security and privacy of customer data. The naming convention for our AWS Regions is indicative of the general geographic location of the Availability Zones and data centers that make-up that AWS Region. Additional detail regarding the general location of data centers is contained in our PCI-DSS report available through AWS Artifact. To learn more, see our AWS Global Infrastructure web page.	OPS 1 Determining Priorities OPS 2 Organization Structure OPS 3 Organization Culture OPS 4 Workload design for Observability OPS 5 Improve Production Flow OPS 6 Mitigate Deployment Risk REL 8 Implementing Change

2. Policy of contracting and management of activities related to the outsourcing of services

The policy that corresponds to be sanctioned by the Board of Directors of the entity, or the body that takes its place, must address at least the following matters:

Requirements	AWS Considerations	Implementation
a) The definition of the governance structure and the procedures to be followed to authorize and manage the outsourcing of services, including the reporting and responsibility lines. **b**) A description of the specific risk assessment tools in this area and their use. **c)** Criteria for defining permitted thresholds or limits or tolerance to inherent and residual risk, as well as mitigation and monitoring instruments and strategies. **d)** Particular procurement criteria, in the case of a supplier that is a related entity. **e)** Elements that are considered by the entity to determine those services that, in its opinion, are associated with significant or strategic activities. **f)** The definition of those activities that can only be outsourced with the approval of the Board of Directors or another instance of the administration that is defined. **g)** Periodicity of review of the policy, especially when there are relevant changes in the risk profile of the institution. **h)** The minimum elements that must be incorporated in the contract for the provision of services.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.

Requirements	AWS Considerations	Implementation
i) Definition of the mechanisms to have prior authorization from each customer, in case the service to be outsourced includes the transmission of data outside the country, which by their nature are subject to the provisions of article 154 of the General Law of Banks, relating to the reservation or bank secrecy. Notwithstanding the foregoing, it should be remembered that outsourced services in Chile are subject to the same obligation of reservation or secrecy as appropriate, to which the entity is subject.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use. The AWS customer can choose the AWS Region or Regions in which their content is located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. As an AWS customer, you maintain ownership of your content, and you select which AWS services can process, store, and host your content. Customers can replicate and back up their content in more than one AWS Region. AWS won't move or replicate customers' content outside of their chosen AWS Region(s) without their agreement, except as necessary to comply with the law.	SEC 7 Data Classification SEC 8 Protection at Rest SEC 9 Protection in Transit
j) Definition of the elements related to risk management that are not applicable to certain types of activities or services that are carried out locally, in accordance with the provisions of Annex No. 4.	**Customer responsibility.** AWS customers are responsible for defining their governance, risk assessment, and operational process models for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.

3. Business continuity

Requirements	AWS Considerations	Implementation
The entity must verify that its critical service providers have appropriate plans that verify the continuity of the contracted services. In the same way, the entity must verify that its critical suppliers check that the services subcontracted by them have appropriate business continuity plans. These plans must be tested at least once a year including, where appropriate, the disaster scenario of their different processing sites, and the entity must become aware of said activity and verify the results obtained. Additionally, the entity must also have plans, equally proven, to verify operational continuity in the event of the contingency of not having such external service.	**Shared responsibility.** Customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS. Customers can utilize the AWS Cloud 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. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances, and store data within multiple geographic AWS Regions as well as across multiple Availability Zones (AZs) within each AWS Region. 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 Data centers are designed to anticipate and tolerate failure while maintaining service levels. In the case of failure, automated processes move customer data traffic away from the affected area. Each AZ is engineered to operate independently with high reliability. AZs are connected to enable you to efficiently architect applications that automatically fail-over between AZs without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of AZs and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. Each AZ is designed as an independent failure zone. This means that AZ are typically physically separated within a metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region).	REL 10 Fault Isolation REL 11 Resiliency implementation REL 12 Testing Reliability REL 13 Disaster Recovery OPS 7 Supporting a Workload OPS 10 Workload and operations events

Requirements	AWS Considerations	Implementation
	In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AZs are each fed through different grids from independent utilities to further reduce single points of failure. AZs are redundantly connected to multiple tier-1 transit providers. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS tests the Business Continuity plan and its associated procedures at least annually to check effectiveness of the plan and the organization readiness to manage the plan. Customers can refer to SOC 2 report in AWS Artifact for further information. Additionally, AWS has obtained ISO 22301:2019 Certification. Alignment with ISO 22301 demonstrates to customers that AWS has an effective Business Continuity Management System (BCMS) in place to support compliance to the only global security and resiliency standard, ISO 22301:2019. AWS's alignment with and independent third-party assessment of this internationally recognized code of practice demonstrates AWS's commitment to the business continuity and resiliency of AWS global services and assures compliance with international standards. Customers can learn more about these topics by downloading: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond, and Disaster Recovery of Workloads on AWS: Recovery in the Cloud	
The entity must have exit plans in the event of breaches of these suppliers, which consider the early termination of the contractual relationship and allow the operation to resume, either on its own account or through another supplier.	**Customer responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use	Not applicable.

Requirements	AWS Considerations	Implementation
The institution must verify that the supplier has a formal and systematic management process in place in the face of incidents that could interrupt or affect the provision of products, services or activities.	**Shared responsibility.** Customers are responsible for defining their operational model based on the AWS services they choose to use. As part of the shared security responsibility model, security events monitoring should be performed by both AWS and AWS customers. AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub, and AWS Config Rules to track, monitor, analyze, and audit events. If these tools identify an event that is analyzed and determined to be an incident, that "qualifying event" can raise an incident and trigger the incident management process and any appropriate response actions necessary to mitigate the incident on the customer side. AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase 2. Recovery Phase 3. Reconstitution Phase To 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 Amazon 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. The Incident Response Test Plan is managed annually, in conjunction with the Incident Response plan. AWS Incident Management planning, testing, and test results are reviewed by third party auditors. Customers can access this information through the SOC 2 report available in AWS Artifact. Customers can learn more about this topic by downloading: AWS Security Incident Response Guide and NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud.	SEC 10 Incident response OPS 7 Supporting a Workload OPS 8 Health of a Workload OPS 9 Health of Operations OPS 10 Workload and operations events

Requirements	AWS Considerations	Implementation
	In addition, 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.	
Processing sites and technological infrastructure that support outsourced services must consider the requirements indicated in Title II of Chapter 20-9 of this Compilation.	**Shared responsibility.** Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS customers can use the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals. AWS Regions are composed of multiple Availability Zones (AZs) that are designed to be independent of each other. Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our AZs are built to be independent and physically separated from one another. By deploying across multiple AZs in a single AWS Region, your workload is better protected against failure of a single (or even multiple) data centers. Each AZ is designed as an independent failure zone. This means that AZs are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Customers can achieve extremely high recovery time and recovery point objectives by using multiple AZs and data replication. AWS Regions are designed to be autonomous, and thus to use a multi-region approach you would deploy dedicated copies of services to each AWS Region. A multi-region approach is common for disaster recovery strategies to meet recovery objectives when one-off large-scale events occur. The most resilient architectures use multiple AWS Regions to achieve greater geographic separation than using a single AWS Region.	REL 10 Fault Isolation REL 11 Resiliency implementation REL 13 Disaster Recovery OPS 7 Supporting a Workload OPS 10 Workload and operations events

Requirements	AWS Considerations	Implementation
	AWS data center's electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS verifies data centers are equipped with back-up power supply available to maintain operations in the event of an electrical failure for critical and essential loads in the facility. AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels. AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule. AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment. AWS Service Level agreements are documented here: AWS Service Level Agreements (SLAs). AWS Compliance Programs empower customers to understand the robust controls in place at AWS to maintain security and data protection in the AWS Cloud. When systems are built in the AWS Cloud, AWS and customers share compliance responsibilities. AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1. Additionally, AWS also has assurance programs that provide templates and control mappings to help customers establish the compliance of their environments running on AWS. For a full list of programs, see AWS Compliance Programs. Reports are available in AWS Artifact.	

4. Security

Of its own information and that of its customers, in the cases that correspond.

Requirements	AWS Considerations	Implementation
The entity must verify that the service provider maintains an information security program that allows it to check the confidentiality, integrity, traceability and availability of its information assets and that of its customers. These conditions must be consistent with the policies and standards adopted by the entity and be incorporated into the contract for the provision of services.	**Shared responsibility.** Customers define their governance, risk assessment, and operational model. AWS has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. AWS management reviews and evaluates the risks identified in the risk management program at least annually. AWS management leads an information security program that identifies and establishes security goals that are relevant to business requirements. Annual evaluations are performed to allocate the resources necessary for performing information security activities within AWS to meet or exceed customer and service specifications. As a customer, you maintain full control of your content that you upload to the AWS services under your AWS account, and responsibility for configuring access to AWS services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (such as AWS Identity and Access Management (IAM), AWS Organizations and AWS CloudTrail). We provide APIs for you to configure access control permissions for the services you develop or deploy in an AWS environment. See this AWS compliance FAQ. Additionally, AWS financial institution customers have the option to enroll in an Enterprise Agreement with AWS. Through an AWS Enterprise Agreement, AWS offers financial institutions regulated by the CMF a contractual framework that might help them satisfy the applicable contractual requirements under the RAN 20-7. For more information about AWS Enterprise Agreements, please contact your AWS representative.	SEC 1 Secure Operations SEC 2 Authentication SEC 3: Authorization and access control SEC 8: Data protection at rest SEC 9: Data protection in transit

Requirements	AWS Considerations	Implementation
	Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 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. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals. There are four AWS SOC Reports available to AWS customers from AWS Artifact: ○ AWS SOC 1 Report ○ AWS SOC 2 Security, Availability & Confidentiality Report ○ AWS SOC 2 Privacy Type I Report ○ AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper. AWS internal and external audits are planned and performed according to the documented audit schedule to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards based criteria includes but is not limited to the ISO/IEC 27001, the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.	

Requirements	AWS Considerations	Implementation
The entity must control and monitor the information security infrastructure provided by the provider, in order to protect the information assets, present in the outsourced critical services, independent of the controls provided by the provider. Likewise, it must control and monitor identity management and access control to information related to these critical services.	**Customer responsibility.** 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. In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user and programmatic access to AWS services and resources. You can apply granular policies, which assign permissions to a user, group, role, or resource. You also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). You can use federation with your existing directory service. For workloads that require systems to have access to AWS, IAM enables secure access through roles, instance profiles, identity federation, and temporary credentials. 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 and where it is stored, used, and protected from disclosure. AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help financial institution customers do this effectively. We do not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. Changes to customer environments can be detected and tracked using AWS Services such as AWS Config to assess, audit, and evaluate the configurations of AWS resources. AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, verify that AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub are enabled for all accounts within your organization.	SEC 2 Authentication SEC 3: Authorization and access control SEC 5: Network protection SEC 6 Compute protection PERF 7 Monitor performance REL 6 Resourcing monitoring

Requirements	AWS Considerations	Implementation
	AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews help you tune automation tools, and continuously iterate. For example, automate responses to events by automating the first investigation step, then iterate to gradually remove human effort with Amazon GuardDuty, a continuous security monitoring service that helps you to identify unexpected and potentially unauthorized or malicious activity in your AWS environment. In addition, 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.	
Communications connections between the entity and the service provider must have a level of encryption that checks the confidentiality and integrity of end-to-end data.	**Shared responsibility.** 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 offers you the ability to add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. These include: Data at rest encryption capabilities available in most AWS services, such as Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker. Flexible key management options, including AWS Key Management Service (AWS KMS), that allow you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your own keys. Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to help satisfy your compliance requirements.	SEC 8: Data protection at rest SEC 9: Data protection in transit

Requirements	AWS Considerations	Implementation
	Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS. In addition, AWS provides APIs for you to integrate encryption and data protection with the services you develop or deploy in an AWS environment. For further information refer to Encrypting Data-at-Rest and -in-Transit, Data Encryption, and How to protect data in transit? AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help verify that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data. Customers can use AWS CloudHSM. AWS CloudHSM is a service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If you need to secure your encryption keys in a service backed by FIPS-validated HSMs, but you do not need to manage the HSM, you might consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, see S3 User Guide - Protecting Data Using Server-Side Encryption.	
The entity must verify that the provider has effective control and protection measures against external attacks that pursue the unavailability of the contracted services, such as, for example, those of denial of services. Additionally, for outsourced critical services, the entity must control the provider's periodic performance of vulnerability assessments of its technological infrastructure and penetration testing.	**Shared responsibility.** AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed on AWS Customer Support Policy for Penetration Testing.	SEC 5: Network protection SEC 6 Compute protection REL 4 Design interactions to prevent failures REL 5 Design interactions to mitigate failures

Requirements	AWS Considerations	Implementation
	AWS utilizes a wide variety of automated monitoring systems designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity and alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. Responses are performed according to incident response processes and procedures. Amazon Web Services takes security very seriously, and investigates all reported vulnerabilities. Customers can report vulnerabilities and security concerns regarding AWS cloud services or open-source projects by submitting a Vulnerability Report. AWS is committed to being responsive and keeping you informed of our progress as we investigate and/or mitigate customers' reported security concerns. Customers receive a non-automated response to their initial contact within 24 hours, confirming receipt of the reported vulnerability. Customers receive progress updates from AWS at least every five US working days. AWS Security performs regular vulnerability scans on the underlying infrastructure, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third-party vendor at least quarterly, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS can validate controls on SOC 2 report available through AWS Artifact. 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 endpoints are tested as part of AWS compliance vulnerability scans.	

Requirements	AWS Considerations	Implementation
	AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS through the AWS Vulnerability Reporting website. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced. All AWS customers benefit from the automatic protections of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your web site or applications. When you use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, you receive comprehensive availability protection against known infrastructure (Layer 3 and 4) attacks. For higher levels of protection against attacks AWS Customers can use AWS Shield Advanced. In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that can affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting.	

Requirements	AWS Considerations	Implementation
The information once processed must be stored and transported in encrypted form, keeping the decryption keys in the possession of the entity. Likewise, the procedures for exchanging keys between the service provider and the institution must be defined, in addition to establishing the roles and responsibilities of the people involved in the administration of security.	**Shared responsibility.** 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 customers can encrypt their content, and we provide customers with the option to manage their own encryption keys. AWS customers choose how their content is secured. AWS offers industry-leading encryption features to protect customers' content in transit and at rest. AWS provides customers options to manage their own encryption keys. These data protection features include: Data encryption capabilities available in over 100 AWS services. Flexible key management options using AWS Key Management Service (AWS KMS), allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys. AWS protects the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help verify that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data. AWS Customers can use AWS CloudHSM service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If you need to secure your encryption keys in a service backed by FIPS-validated HSMs, but you do not need to manage the HSM, you might consider AWS Key Management Service (AWS KMS). For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage. For more information, see S3 User Guide - Protecting Data Using Server-Side Encryption.	SEC 2 Authentication SEC 3: Authorization and access control SEC 5: Network protection SEC 6 Compute protection SEC 8: Data protection at rest SEC 9: Data protection in transit

Requirements	AWS Considerations	Implementation
In the case of processing physical documentation, the entity must have control procedures that verify due compliance with the conditions indicated in this Title. Along with the preceding, procedures must be established to verify the adequate transfer of information to the entity by the supplier, and that the latter in no case maintains information in its possession after the end of the contractual relationship.	**Customer responsibility.** Customers define their governance, risk assessment, and operational model.	Not applicable.

5. Country risk

Requirements	AWS Considerations	Implementation
Services can only be outsourced in jurisdictions that have an investment grade country risk rating. However, the Board of Directors or the instance acting on its behalf might exempt this requirement, to the extent that the country in which the services are outsourced has adequate laws for the protection and security of personal data, and must record the analysis carried out for this purpose. The foregoing, without prejudice to what is indicated in number 2 letter i) of Title III and number 1 letter b) of Title IV of this Chapter.	**Customer responsibility.** AWS customers are responsible for defining their operational process model for managing systems, databases, and services, as well as the risk assessment process they use. As an AWS customer, you maintain ownership of your content, and you select which AWS services can process, store, and host your content. AWS does not access or use your content for any purpose without your consent. AWS never uses customer content or derive information from it for marketing or advertising. The AWS customer can choose the AWS Region or Regions in which their content is located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. Customers can replicate and back up their content in more than one AWS Region. AWS won't move or replicate customers' content outside of their chosen AWS Region(s) without their agreement, except as necessary to comply with the law or a binding order of a governmental body. The naming convention for our AWS Regions is indicative of the general geographic location of the Availability Zones and data centers that make-up that AWS Region. Additional detail regarding the general location of data centers is contained in our PCI-DSS report available through AWS Artifact. To learn more, see our AWS Global Infrastructure web page.	Not applicable.

6. Responsibility for management

Requirements	AWS Considerations	Implementation
Responsibility for overall risk management and control functions shall be maintained by the institution in the country. The foregoing is without prejudice to the fact that in some international entities there are, for the purposes of a consolidated administration of their parent companies, matrix coordination between personnel established abroad and local personnel.	**Customer responsibility.** AWS customers are responsible for defining their operational process model for managing systems, databases, and services, as well as the risk assessment process they use.	Not applicable.
Moreover, in compliance with the provisions of Chapter 20-8 of this Compilation, the institution must immediately communicate to this Superintendence, when appropriate, the relevant operational incidents that affect an outsourced service in the country or abroad.	**Customer responsibility.** AWS Customers are responsible for complying with these requirements from the CMF regarding information security incidents. As part of the shared security responsibility model, security events monitoring should be performed by both AWS and AWS customers. AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, AWS Security Hub, and AWS Config Rules to track, monitor, analyze, and audit events. If these tools identify an event that is analyzed and determined to be an incident, that "qualifying event" can raise an incident and trigger the incident management process and any appropriate response actions necessary to mitigate the incident on the customer side. Customers can learn more about this topic by downloading: AWS Security Incident Response Guide and NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud. In addition, 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.	SEC 4 Security events OPS 4 Workload design for Observability OPS 6 Mitigate Deployment Risk OPS 8 Health of a Workload OPS 9 Health of Operations OPS 10 Workload and operations events REL 6 Resourcing monitoring

7. Access to information by the supervisor

Requirements	AWS Considerations	Implementation
The entity must verify that this Superintendence has permanent access, either through visits to the facilities of the service providers or remotely, to all records, data and information that are processed, maintained and generated through an external provider, whether established in the country or abroad. As a service provider established abroad, special attention must be paid to the legal restrictions of the host country that might prevent the visit of this Superintendence to the provider or access to the information and data mentioned in the previous paragraph. Likewise, as part of risk management, the entity must incorporate within the analysis those aspects related to the legal risks to which the information subject to secrecy or bank reserve established in the General Banking Law is exposed.	**Shared responsibility.** 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. In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user and programmatic access to AWS services and resources. You can apply granular policies, which assign permissions to a user, group, role, or resource. You also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). You can use federation with your existing directory service. For workloads that require systems to have access to AWS, IAM enables secure access through roles, instance profiles, identity federation, and temporary credentials. 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 and where it is stored, used, and protected from disclosure. AWS financial institution customers have the option to enroll in an Enterprise Agreement with AWS. Through an AWS Enterprise Agreement, AWS offers customers a contractual framework that might help them satisfy the applicable contractual requirements, including specific terms that address the CMF's access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative.	Not applicable.

IV. FACTORS TO CONSIDER WHEN OUTSOURCING DATA PROCESSING SERVICES.

The contracting of external data processing services must be supported by the background detailed in Annex No. 2 of this Chapter, in addition to considering the factors indicated in the following.

Additionally, in the evaluation carried out for this purpose by this Agency, on the occasion of its control activities, it is distinguished according to the type of services in question.

1. Geographic location of the provider

Requirements	AWS Considerations	Implementation
a) In-country services When the data processing service, total or partial, is carried out by a company located in the country, the institution must verify that the technological infrastructure and the systems that are used for the communication, storage and processing of data, offer sufficient security to permanently safeguard the continuity of the business, confidentiality, integrity, accuracy and quality of the information. Likewise, it must verify that the conditions of the service guarantee the timely obtaining of any record, data or information that it needs, either for its own purposes or to comply with the requirements of the competent authorities, as is the case of the information that this Superintendence can request at any time. As for the contingency Data Processing Center, it must comply with conditions of location and distance from the main Data Processing Center, which guarantee operational continuity. **b) Services performed abroad**	**Customer responsibility.** The AWS customer can choose the AWS Region or Regions in which their content is located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. Customers can define the workloads' architecture to meet specific geographic or regulatory requirements. Customers can work with their AWS account manager and AWS architect for assistance on architecture definition. AWS services are structured so that a customer maintains effective control of customer content regardless of what AWS Region they use for their content. This allows customers to establish environments that meet specific geographic or regulatory requirements. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances, and store data within multiple geographic AWS Regions as well as across multiple Availability Zones (AZs) within each AWS Region.	OPS 4 Workload design for Observability OPS 6 Mitigate Deployment Risk OPS 8 Health of a Workload OPS 9 Health of Operations OPS 10 Workload and operations events REL 4 Design interactions to prevent failures REL 5 Design interactions to mitigate failures REL 9: Data Backup REL 10 Fault Isolation REL 11 Resiliency implementation REL 12 Testing Reliability REL 13 Disaster Recovery

Requirements	AWS Considerations	Implementation
In the event that the entity outsources data processing services outside the country, it must have at all times the background of the contracted company. In particular, it must maintain those antecedents that support the financial soundness of the service provider and that it maintains quality, safety and appropriate control systems certifications. Additionally, the entity must have the background of the project, the service contract and, in the case of subcontracts with third parties, these must also be incorporated. To safeguard the proper functioning of the financial environment with all its participants, including customers, institutions that carry out activities considered significant or strategic abroad must keep at the disposal of this Superintendence the background contained in Annex No. 2 of this Chapter and comply with the following conditions for the outsourcing of services: **i)** A contingency Data Processing Center located in Chile must be available and demonstrate a recovery time compatible with the criticality of the outsourced service. Likewise, recovery times must be evaluated by the entity at least once a year, both for transactional and Batch processes. In the case of banks that maintain adequate operational risk management in the last evaluation carried out by this Commission, qualified in accordance with the provisions of Chapter 1-13 of this Compilation, the Board of Directors or the body that takes its place might exempt this requirement, when it is verified, through an annual report, that the entity complies, among other aspects, with the adoption of the following preventive measures:	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 Data centers are designed to anticipate and tolerate failure while maintaining service levels. In the case of failure, automated processes move customer data traffic away from the affected area. Each AZ is engineered to operate independently with high reliability. AZs are connected to enable you to efficiently architect applications that automatically fail-over between AZs without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of AZs and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. Each AZ is designed as an independent failure zone. This means that AZs are typically physically separated within a metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AZs are each fed through different grids from independent utilities to further reduce single points of failure. AZs are redundantly connected to multiple tier-1 transit providers. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios.	

Requirements	AWS Considerations	Implementation
a) The Recovery Time Objective (RTO) must be approved by the board based on a business impact analysis (BIA) and risk impact analysis (RIA) that is consistent with the criticality of the outsourced service(s). The preceding must be evaluated and tested at least annually. **b)** That the data processing sites comply with an operating availability time equal to or greater than the provisions of Chapter 20-9 of this Collection. **c)** That the sites are located in different locations that mitigate both geographical risk and political risks. **d)** That in terms of information security, outsourced services are provided in an environment consistent with the policies and standards adopted by the entity. The aforementioned report must be carried out by an independent company of recognized prestige and experience in the evaluation of this type of services. **Special considerations** In the case of banking entities that maintain outsourced services abroad, under the conditions indicated in this paragraph, and that as a result of a new evaluation are qualified in the matter of operational risk in a category of "Unsatisfactory Compliance" or lower, they must inform this Commission about the additional specific measures adopted to verify the proper operation of the services. For those banks that do not have a management rating in the field of operational risk, and that outsource services abroad, all the preventive measures indicated in the preceding is applicable, with the exception of the qualification in this matter.	During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS tests the Business Continuity plan and its associated procedures at least annually to verify effectiveness of the plan and the organization readiness to manage the plan. Customers can refer to SOC 2 report in AWS Artifact for further information. As explained in the “Security and Shared Responsibility” section, cloud security is a shared responsibility. AWS manages security of the cloud, ensuring that AWS infrastructure complies with global regulatory requirements as well as best practices. However, security in the cloud is the responsibility of the customer. This means that customers are responsible for the security programs they deploy to protect their content, environments, applications, systems, and networks in the same way as they do in a local data center. Customers can review and download reports and details about more than 2,600 AWS security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals. There are four AWS SOC Reports available to AWS customers from AWS Artifact: ○ AWS SOC 1 Report ○ AWS SOC 2 Security, Availability & Confidentiality Report ○ AWS SOC 2 Privacy Type I Report ○ AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.	

Requirements	AWS Considerations	Implementation
ii) The institution must carry out the control and monitoring of the outsourced service in the Data Processing Center abroad, especially in the aspects related to information security, business continuity and operating conditions of the processing center. Such activities should be duly substantiated according to the risk management carried out for the specific supplier. The preceding, regardless of the control and monitoring activities carried out by the service provider.	AWS internal and external audits are planned and performed according to the documented audit schedule to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards- based criteria includes but is not limited to the ISO/IEC 27001, the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standard. Additionally, AWS financial institution customers have the option to enroll in an Enterprise Agreement with AWS. Through an AWS Enterprise Agreement, AWS offers customers a contractual framework that might help them satisfy the applicable contractual requirements under the RAN 20-7, including specific terms that address the CMF's access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative. Finally, AWS Customers can review AWS financial information in the Investor Relations portal.	

2. External providers of electronic channels

Requirements	AWS Considerations	Implementation
Institutions that require contracting external services necessary to operate with correspondents, that is, those provided by companies that make available electronic channels and maintain agreements with commercial establishments for the provision of certain financial services by mandate of the entity, must contemplate, in what is applicable, the aspects indicated in Annex No. 1 and keep permanently at the disposal of the Superintendence, those antecedents indicated in Annex No. 3. Additionally, the institution must verify compliance with the provisions of Chapter 1-7 of this Compilation.	**Customer responsibility.** Customers are responsible for complying with these requirements from the CMF.	Not applicable.

V. REINFORCED DILIGENCE FOR CLOUD SERVICES

Requirements	AWS Considerations	Implementation
Cloud computing encompasses the evolution of several areas of information technology, such as telecommunications networks and microprocessors, with virtualization or hardware abstraction being one of the most relevant. Due to the variety of services that can be accessed through the cloud, such as infrastructure, services or even software, there is a change in the dynamics of the risks associated with the current technological models of banking. For the purposes of contracting any type of service through the modality called cloud, the Board of Directors of the entity must pronounce annually on the risk tolerance that it is willing to assume in this type of outsourcing. This pronouncement must consider an analysis of the data to be stored or processed under this modality and its location. Without prejudice to due compliance with the various requirements contained in this Chapter 20-7, financial institutions can outsource their non-critical services to the public or private cloud without additional considerations to those already mentioned in the preceding titles. In the event that the entity evaluates the contracting of a cloud service for an activity considered strategic or critical, this might also be carried out in public or private cloud mode; however, in these cases, the entity (financial institution) must carry out an enhanced diligence of the provider and the service, which has to consider the following:	**Shared responsibility.** Customers define their governance and operational model, as well as the risk assessment process they use. As an AWS Customer, you maintain ownership of your content, and you select which AWS services can process, store, and host your content. The AWS customer can choose the AWS Region or Regions in which their content is located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. Customers can define the workloads' architecture to meet specific geographic or regulatory requirements. Customers can work with AWS account manager and AWS architect for assistance on architecture definition. 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 and where it is stored, used, and protected. 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. The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment. IT standards we comply with are broken out by Certifications and Attestations; Laws, Regulations and Privacy; and Alignments and Frameworks.	OPS 10 Workload and operations events SEC 1 Secure Operations SEC 7 Data Classification SEC 8: Data protection at rest SEC 9: Data protection in transit

Requirements	AWS Considerations	Implementation
The provider has recognized prestige and experience in the service it provides. The contracted supplier has independent certifications, internationally recognized, in terms of information security management, business continuity and the quality of services that collect the best practices in force. Service outsourcing contracts are directly between the contracting institution and the suppliers, in order to minimize the risks that the role of intermediary in this type of services could bring. The entity (financial institution) has legal reports regarding the regulation on privacy and access to information existing in jurisdictions where the service is being carried out, and has evaluated the resolution of legal contingencies in the jurisdictions in which it operates. The entity (financial institution) has verified that the service provider makes audit reports associated with the services provided and these reports are available, to be consulted at any time by the contracting entity and the Superintendence, in the matters that are pertinent. Verify that the provider has adequate security mechanisms, both physical and logical, that allow isolating the components of the cloud infrastructure that the entity shares with other customers of the provider, in order to prevent information leaks or events that can affect the confidentiality and integrity of the entity's data. Identify data that by its nature and sensitivity must have strong encryption mechanisms.	Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. AWS customers remain responsible for complying with applicable compliance laws, regulations and privacy programs. AWS Compliance Program include, but are not limited to AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017, 22301, and 27018 certifications and PCI DSS compliance reports. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications and PCI DSS compliance reports. Reports and certifications can be downloaded using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. AWS financial institution customers have the option to enroll in an Enterprise Agreement with AWS. Through an AWS Enterprise Agreement, AWS offers customers a contractual framework that might help them satisfy the applicable contractual requirements under the RAN 20-7, including specific terms that address the CMF´s access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative. Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualized operational environments to customers (that is, Amazon EC2) verify that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure through hypervisors and instance isolation.	

Requirements	AWS Considerations	Implementation
	Different instances running on the same physical machine are isolated from each other through the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. Packets must pass through this layer; thus, an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms. Customer instances have no access to physical disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data using traditional filesystem encryption mechanisms, or, in the case of Amazon Elastic Block Store (Amazon EBS) volumes, by enabling AWS-managed disk encryption.	

VI. REVIEWS OF THIS SUPERINTENDENCE

Requirements	AWS Considerations	Implementation
In its inspection visits, this Superintendence examines the risk management carried out by the entity on the outsourcing of services, as part of the evaluations performed with in Chapter 1-13 of this Compilation. In the event of non-compliance with these regulations, especially by those entities that have outsourced significant or strategic activities abroad or that expose them to relevant operational risks, this Agency might require that the services be carried out in the country, or be managed internally by the entity, as appropriate. In consideration of the preceding, the entity must keep permanently updated a plan that makes it possible to comply with these possible requirements.	**Customer responsibility.** 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 define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. The AWS customer can choose the AWS Region or Regions in which their content is located and can choose to deploy their AWS services exclusively in a single AWS Region if preferred. Customers can define the workloads' architecture to meet specific geographic or regulatory requirements. Customers can work with their AWS account manager and AWS architect for assistance on architecture definition. AWS services are structured so that a customer maintains effective control of customer content regardless of what AWS Region they use for their content. This allows customers to establish environments that meet specific geographic or regulatory requirements. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances, and store data within multiple geographic AWS Regions as well as across multiple Availability Zones (AZs) within each AWS Region. 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 Data centers are designed to anticipate and tolerate failure while maintaining service levels. In the case of failure, automated processes move customer data traffic away from the affected area.	Not applicable.

Requirements	AWS Considerations	Implementation
	Each AZ is engineered to operate independently with high reliability. AZs are connected to enable you to efficiently architect applications that automatically fail-over between AZs without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of AZs and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. Each AZ is designed as an independent failure zone. This means that AZs are typically physically separated within a metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AZs are each fed through different grids from independent utilities to further reduce single points of failure. AZs are redundantly connected to multiple tier-1 transit providers. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS tests the Business Continuity plan and its associated procedures at least annually to verify effectiveness of the plan and the organization readiness to manage the plan. Customers can refer to SOC 2 report in AWS Artifact for further information. The AWS Compliance Program helps customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance Enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment.	

Requirements	AWS Considerations	Implementation
	IT standards we comply with are broken out by Certifications and Attestations; Laws, Regulations and Privacy; and Alignments and Frameworks. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance. AWS customers remain responsible for complying with applicable compliance laws, regulations and privacy programs. AWS Compliance Program include, but are not limited to AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017, 22301, and 27018 certifications and PCI DSS compliance reports. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications and PCI DSS compliance reports. Reports and certifications can be downloaded using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. AWS services allow for the export of content by customers on demand, using the AWS Management Console, APIs, and other input methods. For example, AWS Snowball provides devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud. For more information about migrating data in and out of AWS, see: Migration & Transfer on AWS.	

ANNEX No 1. MINIMUM ASPECTS THAT MUST BE CONSIDERED FOR THE OUTSOURCING OF SERVICES

Requirements	AWS Considerations	Implementation
1. Risk assessment. Before deciding on the outsourcing of an activity, an evaluation must be carried out, which considers all the agents involved regarding the risks that this decision incorporates into the institution, as well as the amount of risk committed due to the amounts paid to the external company, volume of transactions to be processed, criticality of the contracted service, concentration of services with the same supplier, concentration of the financial sector in a specific supplier, among others. In this evaluation, the opinion of the area in charge of the operational risk management of the audited entity must be considered, which must be duly supported.	**Customer responsibility.** Customers define their governance and operational model, as well as the risk assessment process they use. AWS Customers are responsible for complying with these requirements from the CMF.	Not applicable.
2. Selection of the service provider. The institution must evaluate the proposals received according to its requirements and carry out a due diligence that supports the information received from potential suppliers. In the event that a service is contracted with a related entity, the economic conditions must comply with principles of transparency and fairness, aspects that must be defined in the policy that regulates the outsourcing of services.	**Customer responsibility.** Customers define their governance and operational model, as well as the risk assessment process they use. AWS Customers are responsible for complying with these requirements from the CMF.	Not applicable.
3. Contract. The institution must verify that the contract clearly defines the rights and obligations of both parties, containing agreements of clear and measurable levels of the contracted services, early termination clauses of the contractual relationship, as well as an appropriate pricing method for the specific contract. In case more than one service is purchased for a single price, the detail of the charge for each of these services must be taken.	**Shared responsibility.**	SEC 1 Secure Operations SEC 7 Data Classification SEC 10 Incident response REL 11 Resiliency implementation REL 13 Disaster Recovery

Requirements	AWS Considerations	Implementation
Business continuity and information security clauses must also be included, especially that which refers to the ownership and confidentiality of information, both its own and that of its customers; restrictions on the use of software; secure deletion of customer data, where applicable; in addition to establishing a permanent authorization that allows both this Superintendence and the audited entity to examine in situ, or remotely, as provided, at any time, all aspects related to the contracted service. Additionally, the institution should consider veto clauses in the selection of outsourcing of third parties by the main supplier. Contractually, everything related to the suitability and responsibility of the personnel of the company providing the service must be clearly established, as well as all the legal and labor aspects that prevail in the country or abroad, applicable to these contracts. Finally, all contracts, subcontracts and their respective annexes must be in Spanish, or translated into this language, and with the corresponding rubrics of the parties.	AWS financial institution customers have the option to enroll in an Enterprise Agreement with AWS. Through an AWS Enterprise Agreement, AWS offers customers a contractual framework that might help them satisfy the applicable contractual requirements under the RAN 20-7, including specific terms that address the CMF´s access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative.	
4. Permanent control. **From the provider:** The institution must monitor the performance of the provider and possible changes in the requirements of the institution during the term of the contract. The control should include at least: the knowledge and analysis of the latest financial statement of the supplier and aspects such as the observation of the general control environment of the external company.	**Customer responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. Through an AWS Enterprise Agreement, AWS offers customers a contractual framework that might help them satisfy the applicable contractual requirements, including specific terms that address the CMF's access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative.	OPS 5 Improve Production Flow OPS 7 Supporting a Workload OPS 9 Health of Operations OPS 10 Workload and operations events

Requirements	AWS Considerations	Implementation
Of the service: The institution must have procedures that allow it to control compliance with the clauses stipulated in the contracts. Monitoring should include at least: service level agreements, contractual arrangements, management of the operational risk associated with the contracted service, and possible changes due to the external environment. Additionally, the existence and sufficiency of the procedures for transfer to production and escalation of incidents must be evaluated and tested, at least annually; as well as define and control the relevant milestones of each of these 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. AWS Service Level agreements are documented here: AWS Service Level Agreements (SLAs). AWS Customers can review AWS's public financial information in the Investor Relations portal.	

ANNEX No 2. ADDITIONAL BACKGROUND FOR OUTSOURCING DATA PROCESSING SERVICES

I. Overview

Requirements	AWS Considerations	Implementation
Governance structure defined between the entity and the supplier, clearly identifying its strategic, tactical and operational level, both in the stage of project development and relationship in regime. Detailed cost structure of current and post-external data processing (for the same items considered).	**Customer responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. AWS Support provides a mix of tools and technology, people, and programs designed to proactively help you optimize performance, lower costs, and innovate faster. We save time for your team by helping you to move faster in the cloud and focus on your core business. AWS Support plans can be found here. For further information on pricing models please refer to AWS Pricing site.	Not applicable.

II. Project Information

Requirements	AWS Considerations	Implementation
Detailed scope of the external processing service. Detailed identification of the business servers and applications that are processed externally and those that remain in the institution. Supporting documents of the external processing project, which must be consistent with the project management methodology adopted by the entity. Detail of the items that are considered in the respective tariff agreement. Risk analysis and assessment report carried out by an independent entity. This report must include the risk matrix of the project, which must contemplate at least, the identification of the outsourced processes, the identification of the sources and risk factors that affect them, the inherent risk, the impact and probability of occurrence, and an evaluation of the design and operation of the controls for the determination of the resulting residual risk. Technical and financial evaluation of the project. Evaluations carried out for the selection of suppliers. Detail of the transfer methodology used if applicable (hardware, software and telecommunications). Methodology of certification of tests and simulations. Acceptance criteria established for each sub-stage and activities that make up the project	**Shared responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. As an AWS customer, you maintain ownership of your content, and you select which AWS services can process, store, and host your content. AWS does not access or use your content for any purpose without your consent. For information on pricing models please refer to AWS Pricing site. For more information about AWS Enterprise Agreements and AWS pricing, please contact your AWS representative. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 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. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console.	OPS 7 Supporting a Workload OPS 9 Health of Operations
Service contract (including all annexes) and in the case of subcontracts with third parties these must also be incorporated.	**Shared responsibility.** AWS financial institution customers have the option to manage an Enterprise Agreement with AWS.	Not applicable.

Requirements	AWS Considerations	Implementation
Information security and business continuity policies of the service provider.	**Shared responsibility.** As explained in the "Security and the AWS Shared Responsibility Model" section, cloud security is a shared responsibility. AWS manages security of the cloud, ensuring that AWS infrastructure complies with global regulatory requirements as well as best practices. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 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. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. Customers can utilize the AWS Cloud to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios.	SEC 1 Secure Operations SEC 4 Security events SEC 7 Data Classification SEC 8 Protection at Rest SEC 9 Protection in Transit SEC 10 Incident response OPS 7 Supporting a Workload OPS 8 Health of a Workload OPS 10 Workload and operations events REL 9: Data Backup REL 11 Resiliency implementation REL 13 Disaster Recovery

Requirements	AWS Considerations	Implementation
	During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS tests the Business Continuity plan and its associated procedures at least annually to verify effectiveness of the plan and the organization readiness to manage the plan. Customers can refer to SOC 2 report in AWS Artifact for further information. In addition to that AWS has obtained ISO 22301:2019 Certification. Alignment with ISO 22301 demonstrates to customers that AWS has an effective Business Continuity Management System (BCMS) in place to support compliance to the only global security and resiliency standard ISO 22301:2019. AWS's alignment with and independent third-party assessment of this internationally recognized code of practice demonstrates AWS's commitment to the business continuity and resiliency of AWS global services and assures compliance with international standards.	
Description, background and detailed technical characteristics of the production site and contingency of the service provider and the certifications it has.	**Shared responsibility.** Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. 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 Data centers are designed to anticipate and tolerate failure while maintaining service levels. In the case of failure, automated processes move customer data traffic away from the affected area.	OPS 1 Determining Priorities OPS 7 Supporting a Workload OPS 8 Health of a Workload OPS 9 Health of Operations OPS 10 Workload and operations events REL 6 Resourcing monitoring REL 9: Data Backup REL 10 Fault Isolation

Requirements	AWS Considerations	Implementation
	Each AZ is engineered to operate independently with high reliability. AZs are connected to enable you to efficiently architect applications that automatically fail-over between AZs without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of AZs and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability. Each AZ is designed as an independent failure zone. This means that AZs are typically physically separated within a metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AZs are each fed through different grids from independent utilities to further reduce single points of failure. AZs are redundantly connected to multiple tier-1 transit providers. For further information please see Our Controls site. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 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. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console.	REL 11 Resiliency implementation REL 12 Testing Reliability REL 13 Disaster Recovery
14. Detailed GANTT chart of the outsourcing project.	**Customer responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.	Not applicable.

Requirements	AWS Considerations	Implementation
15. Process and tools that allow the entity (financial institution) to control the application of its policies and good practices in the company providing the service.	**Shared responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use The AWS Compliance Programs help customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals. The AWS Well-Architected Framework helps customers build secure, high-performing, resilient, and efficient infrastructure possible for their applications. The framework provides a consistent approach for customers to evaluate architectures and provides guidance to implement designs that scale with your application needs over time. AWS customers have complete control over which services they use and whom they empower to access their content and services, including what credentials are 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 Customers can secure their workloads and applications in the cloud using AWS Security, Identity, and Compliance services: AWS Identity Services enable customers to securely manage identities, resources, and permissions at scale.	SEC 1 Secure Operations SEC 2 Authentication SEC 3: Authorization and access control SEC 4 Security events SEC 5: Network protection SEC 6 Compute protection

Requirements	AWS Considerations	Implementation
	AWS Compliance services give customers a comprehensive view of their compliance status and continuously monitors their environment using automated compliance checks based on the AWS best practices and industry standards. AWS Network and application protection services enable customers to enforce fine-grained security policies at network control points across their organization. AWS services help customers inspect and filter traffic to prevent unauthorized resource access at the host-, network-, and application-level boundaries.	
16. Process and tools that allow the entity (financial institution) to control compliance with the levels of services committed in the contract signed.	**Customer responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. The AWS Well Architected Framework helps customers build secure, high-performing, resilient, and efficient infrastructure possible for their applications. The framework provides a consistent approach for customers to evaluate architectures, and provides guidance to implement designs that scale with your application needs over time. The AWS Compliance Programs help customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals AWS Customers can use these AWS services to monitor performance.	OPS 8 Health of a Workload OPS 9 Health of Operations OPS 10 Workload and operations events REL 6 Resourcing monitoring PERF 7 Monitor performance

Requirements	AWS Considerations	Implementation
	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. Amazon CloudWatch is a monitoring service for AWS Cloud resources and the workloads that run on AWS. AWS Customers can use CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. CloudWatch can monitor AWS resources such as EC2 instances and Amazon Relational Database Service (Amazon RDS) DB instances, as well as custom metrics generated by customers' workloads and services, and any log files your applications generate. Customers can use CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health. You can use these insights to react quickly and keep your workload running smoothly. Customers can learn more about this topic in: Monitoring, AWS User Engagement Service Level Agreement, AWS Service Level Agreements (SLAs).	

Requirements	AWS Considerations	Implementation
17. Organizational structure that is responsible for the maintenance of hardware, software and communications, especially at the beginning of the external process.	**Shared responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule. AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. AWS's asset owner maintenance procedures are carried out by utilizing a proprietary tool with specified checks that must be completed according to the documented maintenance schedule. Third party auditors test AWS's asset management controls by validating that the asset owner is documented and that the condition of the assets is visually inspected according to the documented asset management policy. The AWS Compliance Programs help customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.	OPS 8 Health of a Workload OPS 9 Health of Operations OPS 10 Workload and operations events REL 6 Resourcing monitoring PERF 7 Monitor performance

Requirements	AWS Considerations	Implementation
18. Policies and procedures that are used for the maintenance of operational and commercial software, both for those that are evolutionary and corrective in nature.	**Shared responsibility.** Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. As explained in the "Security and Shared Responsibility" section, cloud security is a shared responsibility. AWS manages security of the cloud, ensuring that AWS infrastructure complies with global regulatory requirements as well as best practices. However, security in the cloud is the responsibility of the customer. This means that customers are responsible for the security programs they deploy to protect their content, environments, applications, systems, and networks in the same way as they do in a local data center. The AWS Well-Architected Framework helps customers build secure, high-performing, resilient, and efficient infrastructure possible for their applications. The framework provides a consistent approach for customers to evaluate architectures and provides guidance to implement designs that scale with your application needs over time. AWS can schedule events for customers' instances, such as a reboot, stop/start, or retirement. These events do not occur frequently. If one of the customers' instances are affected by a scheduled event, AWS sends an email to the email address that's associated with the customers' AWS account prior to the scheduled event. The email provides details about the event, including the start and end date. Depending on the event, AWS customer might be able to take action to control the timing of the event. AWS also sends an AWS Health event, which the customer can monitor and manage by using CloudWatch Events. For more information about monitoring AWS Health events with CloudWatch, see Monitoring AWS Health events with CloudWatch Events.	OPS 10 Workload and operations events OPS 11 Operations evolution

Requirements	AWS Considerations	Implementation
19. Business continuity plan that the institution adopts in the event of a contingency that prevents processing by the supplier or those subcontracted by it. 20. Contingency plans foreseen to maintain the operational continuity of the contracting entity in the event of failures in the communication or storage of information.	**Shared responsibility.** Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic AWS Regions as well as across multiple Availability Zones (AZs) within each AWS Region. The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement. AWS tests the Business Continuity plan and its associated procedures at least annually to check effectiveness of the plan and the organization readiness to manage the plan. Customers can refer to the SOC 2 report in AWS Artifact for further information.	REL 2 Network topology plan REL 3 Architecture design REL 4 Design interactions to prevent failures REL 7 Design to adapt to changes in demand REL 13 Disaster Recovery

Document revisions

Date	Description
November 2023	Initial draft.
February 2024	First publication.