Guide to Financial Services Regulations in Peru

Resolución S.B.S. 504-2021

September 2024

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 Peru regulated by the Superintendence of Banks, Insurance, and Pension Fund Administrators (Superintendencia de Banca, Seguros y Administradoras de Fondo de Pensiones or S.B.S.) need to comply with Regulations for the Management of Information Security and Cybersecurity (Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad or S.B.S. 504-2021) as they adopt the Amazon Web Services (AWS) Cloud. S.B.S. 504-2021 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 AWS 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 S.B.S. that regulated financial institutions can consider when adopting AWS.

Introduction

The Superintendence of Banks, Insurance, and Pension Fund Administrators (Superintendencia de Banca, Seguros y Administradoras de Fondo de Pensiones or S.B.S.) is Peru's primary authority responsible for the regulation and supervision of financial, insurance, and private pension institutions.

The S.B.S. issued the Regulations for the Management of Information Security and Cybersecurity (*Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad* or S.B.S. 504-2021) in 2021 to update the regulatory framework on information security for institutions regulated by the S.B.S. through the approval of a new regulation, complementary to the Regulations for Operational Risk Management, taking into account international standards and good practices on information security, including those published by the National Institute of Standards and Technology and the ISO/IEC family of standards.

Regulation S.B.S. 504-2021 includes specific contractual, operational, and technical requirements with which regulated financial institutions must comply when outsourcing Information Technology (IT) services to cloud service providers. Further, Regulation S.B.S. 504-2021 was amended by Regulation S.B.S. 03797-2023, Resolution S.B.S. 03240-2023, and Resolution S.B.S. 02286-2024, among others. For the purposes of this guide, when referring to Regulation S.B.S. 504-2021 this reference will include the said amendments.

This guide is a resource to help financial institutions in Peru understand the technical and operational requirements that might apply to them under S.B.S. 504-2021 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 S.B.S. 504-2021.

A full analysis of S.B.S. 504-2021 is beyond the scope of this guide. However, the following sections address the primary considerations that occur in our interactions with financial institutions in Peru and provide information that financial institutions can use to help them understand their responsibilities under S.B.S. 504-2021.

- **Security and shared responsibility:** financial institutions need to understand the AWS Shared Responsibility Model before evaluating the specific technical and operational requirements outlined in S.B.S. 504-2021. 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. AWS 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 S.B.S. 504-2021.
- **Considerations on S.B.S. 504-2021:** This section sets out common considerations for financial institutions that use AWS as they consider some of the key technical and operational requirements under S.B.S. 504-2021 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 Requirements under S.B.S. 504-2021.

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 S.B.S. 504-2021. AWS manages the 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 AWS 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.

AWS customers must carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides flexibility and customer control to workloads. As shown in Figure 1, this differentiation of responsibility is commonly referred to as security *of* the cloud versus security *in* the cloud.

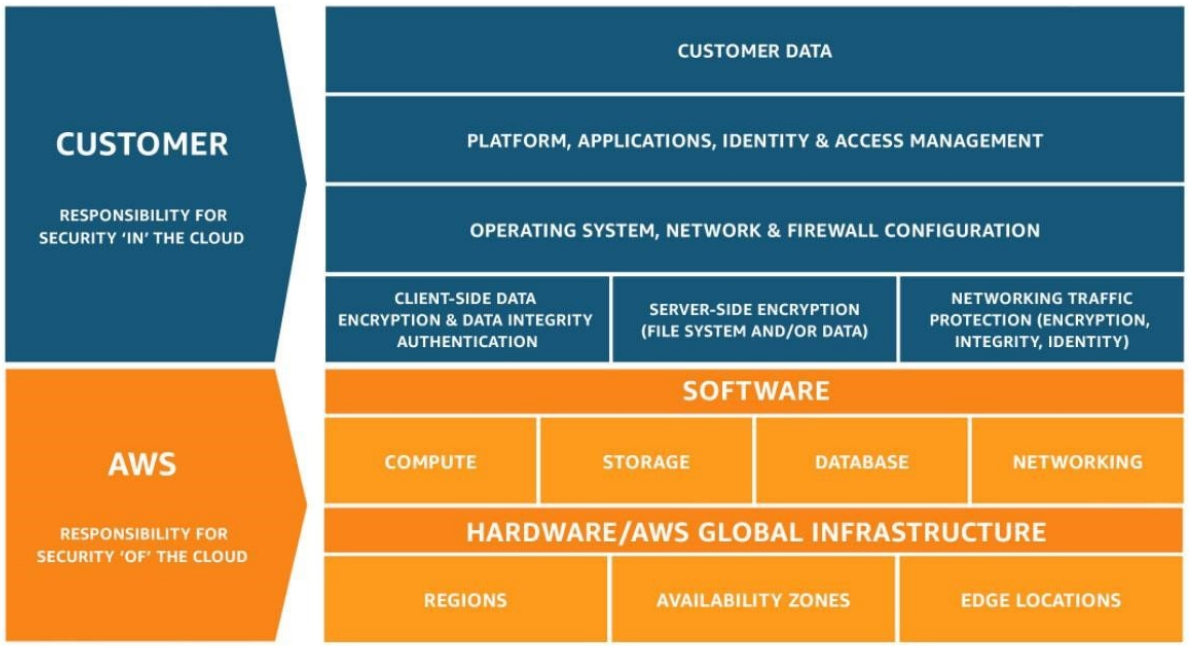

Figure 1 – The AWS Shared Responsibility Model

AWS responsibility - security of the Cloud: AWS is responsible for protecting the infrastructure that runs the AWS services. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS services.

Customer responsibility - security in the Cloud: Customer responsibility is determined by the AWS 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) 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 updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

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

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

The AWS Shared Responsibility Model also extends to IT controls. The responsibility to operate the IT environment is shared between AWS and its customers, and so is the responsibility for the management, operation, and verification of IT controls. AWS can reduce the administrative load on customers by managing the controls associated with

the physical infrastructure deployed in the AWS environment that might 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 might 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 that 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 are applicable to cloud personally identifiable information (PII). It also provides a set of additional controls and associated guidance intended to address 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 27701** Specifies requirements and guidelines to establish and continuously improve the Privacy Information Management System (PIMS), including processing of Personally Identifiable Information (PII). It is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management providing a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processors and controllers, not addressed by the existing ISO/IEC 27002 control set. For more information, or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.
- **ISO 22301**: Specifies the structure and requirements to implement, maintain, and improve a business continuity management system (BCMS) to protect against, reduce the likelihood of the occurrence of, prepare for, respond to, and recover from disruptions when they arise. Compliance to this standard provides assurance on AWS commitment to business continuity and resiliency of AWS services. For more information or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.
- **ISO 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 so 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. 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 might be relevant to a customer's internal controls over financial reporting, in addition to information for the assessment of the effectiveness of internal controls over financial reporting.
    - **SOC 2**: Provides customers and their service users that have 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 that have a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality, without disclosing AWS internal information.

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, AWS Artifact is designed to provide 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 and Communities offer 24x7 access to customer service, documentation, whitepapers, and support forums.

- AWS Trusted Advisor is designed to provide seven core Trusted Advisor checks and guidance to provision resources following best practices to increase performance and improve security.
- AWS Personal Health Dashboard is designed to provide a personalized view of the health of AWS services, and alerts when customer 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 consists 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. AWS customers can learn more about these topics by downloading our whitepaper Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

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

Contractual considerations on S.B.S. 504-2021

The focus of this guide is S.B.S. 504-2021, which regulates the information security and cybersecurity practices of regulated financial institutions when outsourcing services, including cloud services; and is complementary to the Regulations for Operational Risk Management (S.B.S. 2116-2009).

Subchapter IV - outsourcing

The S.B.S. allows financial institutions to outsource IT services to third-party cloud services providers operating in Peru or abroad. The financial entity must provide documentation supporting the requirements detailed in Articles 22, 23, and 24 to the S.B.S. no later than thirty (30) calendar days after outsourcing the service.

Further, according to article 25 of S.B.S. 504-2021, in case of cloud services provided by third parties from abroad and said services present limitations to comply with the requirements established in paragraph 24.2 of article 24, the financial entity must request prior authorization from the S.B.S. to contract said service, which will be responded to by the S.B.S. within sixty (60) business days of submitting the approval request. The financial entity will include the legal support of the identified limitations and a proposal to implement measures to cover for those limitations. The approval only applies to a specific service provider and the city and country where the services are rendered.

Article 24 - regulatory supervision, audit, and inspection

Financial institutions must verify that the S.B.S., the internal audit team, and the external audit firm have adequate access to information, at reasonable times and upon request only. In addition, the financial institution must verify annually that the data processing service provider has information security controls, in accordance with current information security regulations, as applicable to the service provided. This can be supported by independent reports and audit reports that include within their scope the verification of such controls.

For cloud services, to comply with what is required in the previous paragraph, the financial institution must demonstrate annually that the provider maintains current ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 certifications, and that it has a

SOC 2 type 2 report or other equivalents, relevant to the services provided and to the area or region from which the services are provided.

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 S.B.S. a contractual framework that helps them satisfy applicable contractual requirements under the S.B.S. 504-2021 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.

Article 15 - security incidents

Financial institutions must implement the information security and cybersecurity functions and have a multidisciplinary cybersecurity incident management team, which must be able to implement the cybersecurity plan, its procedures, and its governance.

Financial institutions must report to the S.B.S., as soon as it is detected, the occurrence of a cybersecurity incident that has a significant verified or presumed adverse impact such as:

a. Loss or theft of company or customer information.

b. Internal or external fraud.

c. Negative impact on the company's image and reputation.

d. Interruption of operations.

The financial institution must carry out a forensic analysis to determine the causes of the incident and take measures for its management. The report resulting from this analysis must be available to the S.B.S., and must have executive content and the corresponding technical detail.

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. 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.

Getting started

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

For financial institutions in Peru, the next steps are:

- 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, 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 AWS customers in their efforts to implement architecture, products, and services in compliance with applicable technical and operational requirements under S.B.S. 504-2021.

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 in aligning with compliance objectives for regulated workloads on AWS. These features can help 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 secure, high-performing, resilient, and efficient infrastructure for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help 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 can consider when using AWS services and specifically, applying the Shared Responsibility Model to their regulatory requirements. AWS customers 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 conformance to NIST CSF risk management practices (that is, security of the cloud) of AWS offerings. Financial institutions can use NIST CSF and AWS resources to support their risk management frameworks.

For more information, refer to the Security Learning whitepapers.

Appendix: AWS considerations on requirements under S.B.S. 504-2021

The following sections list key technical and operational requirements identified in S.B.S. 504-2021 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 AWS 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:

- **Summary of requirements:** Summarizes the requirements identified in S.B.S. 504-2021.
- **AWS Considerations:** Explains the considerations for addressing the requirements identified in S.B.S. 504-2021. 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.

CHAPTER II. INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT SYSTEM (ISMS-C)

SUBCHAPTER I. GENERAL FRAMEWORK OF THE INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT SYSTEM (ISMS-C)

Article 10. Objectives and requirements of the SGSI-C. The objectives of the SGSI-C are the following:

Summary of requirements	AWS Considerations	Implementation
1. Identify information assets, analyze the threats and vulnerabilities associated with them, and formulate programs and measures to reduce the possibility of incidents in: **a)** The design and implementation of new products and processes, projects and operational changes. **b)** Information security obligations that derive from regulatory provisions, internal regulations and contractual agreements. **c)** Relationships with third parties, in the broadest sense, including service providers and subcontracting relationships.	**Customer responsibility** AWS customers are responsible for identifying, assessing, and mitigating risks to their information assets as part of their overall security program. **a)** AWS provides the AWS Well-Architected Framework to help customers design secure, high-performing, resilient, and efficient architectures for their applications. Customers can use services such as AWS Config, AWS Service Catalog, and AWS CloudFormation to automate the secure deployment and configuration of new resources. AWS offers a comprehensive set of security services such as AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC), AWS WAF, AWS Shield, Amazon GuardDuty that customers can use to build security controls. **b)** AWS customers are responsible for understanding and meeting their regulatory, contractual, and internal information security requirements. AWS provides a wide range of compliance programs, reports, and features to help customers demonstrate compliance. The AWS Financial Services Enterprise Agreement includes terms to help financial institutions address regulatory and legal requirements.	OPS 5 - Improve Production Flow OPS 6 - Mitigate Deployment Risk OPS 7 - Supporting a Workload PERF 1 - Select a High-Performant Architecture PERF 2 - Monitor Performance REL 4 - Design Interactions to Prevent Failures

Summary of requirements	AWS Considerations	Implementation
d) Any other activity that, at the company's discretion, exposes its information assets for internal or external reasons.	The AWS Financial Services Enterprise Agreement offers financial institution customers regulated by the S.B.S. a contractual framework that helps them satisfy applicable contractual requirements under the S.B.S. 504-2021, 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. **c)** AWS customers maintain full control and ownership of their data on AWS, including when using third-party software or services. AWS offers capabilities such as AWS Organizations and AWS Service Catalog to help customers manage and control access for third parties. Customers can use AWS Config and AWS CloudTrail to monitor third-party access and activities in their AWS environment. **d)** AWS has no insight into the specific data or information assets that customers choose to store, and customers retain full control over data protection. Customers can use a variety of AWS security services such as AWS Key Management Service (AWS KMS), AWS CloudHSM, Amazon S3 encryption to help protect their data based on its sensitivity and risk profile. AWS provides customers the ability to audit, monitor, and respond to security events across their entire AWS environment.	
2. Periodically review the scope and effectiveness of the minimum controls indicated in Article 12 of these Regulations and have capabilities to detect, respond and recover from information security incidents.	**Shared responsibility** AWS customers are responsible for defining their operational model based on the AWS services they choose to use. Security events are monitored by both AWS and AWS customers as part of the shared responsibility model. AWS customers can use the security visibility, control, and resilience capabilities provided by AWS to assess and improve their security posture, as well as prepare for, and respond to security incidents. AWS customers can use AWS Artifact to access a wide range of security and compliance reports, including SOC, ISO, and PCI audits, to validate the security controls in place within the AWS environment. AWS undergoes regular independent audits and assessments to verify the design and operating effectiveness of its security controls. Customers can review these results through AWS Artifact.	SEC 1 - Secure Operations SEC 11 - Verification of Controls SEC 10 - Incident Response OPS 9 - Health of Operations OPS 10 - Workload and Operations Events REL 12 - Testing Reliability REL 13 - Disaster Recovery

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for regularly reviewing the security controls they have implemented on top of AWS, such as access policies, network configurations, and data protection measures. AWS provides customers the ability to perform their own security assessments and penetration testing against their AWS resources. *Incident Detection, Response and Recovery:* AWS has implemented a formal, documented incident response policy and program to manage security events that might impact the AWS infrastructure. AWS customers can use AWS security services such as AWS CloudTrail, Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub to detect, investigate, and respond to security incidents in their own environments. AWS provides customers the ability to implement robust backup and disaster recovery strategies using cross-region replication, snapshots, and other data protection features. AWS maintains a comprehensive Business Continuity Plan and tests it annually to verify operational resilience and the ability to recover from large-scale events.	
3. Establish the existing relationship with the emergency, crisis and continuity plans established as provided in the regulations.	**Shared responsibility** AWS customers are responsible for developing their own business continuity and disaster recovery plans for their applications and workloads running on AWS. By aligning their emergency, crisis, and continuity plans with the security and resilience capabilities of AWS, customers can establish a comprehensive approach to prepare for, respond to, and recover from disruptive events. AWS customers can use the redundancy and resilience of the AWS global infrastructure to build highly available and fault-tolerant applications. *Emergency and Crisis Response:* AWS has a comprehensive Incident Response Plan that outlines the processes and procedures for detecting, analyzing, containing, eradicating, and recovering from security incidents that might impact the AWS infrastructure and services. The AWS Incident Response Plan is supported by regular testing and simulations to verify its effectiveness and drive improvement.	OPS 9 - Health of Operations OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for developing their own incident response plans that integrate with the security monitoring, investigation, and mitigation capabilities available in AWS services such as AWS CloudTrail, Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub. *Business Continuity Planning:* AWS has a robust Business Continuity Plan that identifies potential disruptive events and outlines the steps to be taken before, during, and after an incident to maintain service availability. The AWS Business Continuity Plan is supported by measures to avoid and lessen environmental disruptions, including the use of redundant power, connectivity, and data center infrastructure. AWS tests its Business Continuity Plan annually through various simulation exercises to validate its effectiveness and the organizational readiness to run the plan. AWS customers can refer to the SOC 2 report in AWS Artifact for further information. AWS customers are responsible for properly implementing contingency planning, training, and testing for their systems on AWS. Customers can utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. AWS supports Disaster Recovery (DR) architectures. 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. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of 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. AWS has a global infrastructure of Regions and AZs, allowing customers to architect applications for high availability and resilience across geographic locations.	

Summary of requirements	AWS Considerations	Implementation
	Each AZ is engineered to operate independently with high reliability. AZs are connected to enable applications to fail-over between AZs. Highly resilient systems, and therefore service availability, is a function of the system design and AWS customers can achieve short recovery time and recovery point objectives, as well as high levels of service availability using AZs and data replication. 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. AWS provides customers the ability to implement robust backup and disaster recovery strategies using cross-region replication, snapshots, and other data protection features. Services such as AWS Backup, and AWS Outposts enable data protection and migration. AWS has obtained ISO 22301 certification, demonstrating an effective business continuity management system to support customer resilience requirements.	

Article 11. Scope of the SGSI-C.

Summary of requirements	AWS Considerations	Implementation
The scope of the SGSI-C must include organizational functions and units, existing physical locations, technological and communications infrastructure, as well as the perimeter of control associated with relationships with third parties, which are under the company's responsibility, in accordance with the provisions established on subcontracting in the Corporate Governance and Integral Risk Management Regulations.	**Customer responsibility** AWS customers define their governance, risk assessment, and operational models, and can do so based on the AWS services and products they use. *Organizational Functions and Units:* AWS provides a wide range of security services and features that can be used across an organization's different functions and units. Customers maintain full control over user access, permissions, and security configurations within their AWS environment through services such as AWS Identity and Access Management (IAM), AWS Organizations, and AWS Security Hub. *Physical Locations:* AWS has a global infrastructure of Regions and Availability Zones (AZs), allowing customers to architect their applications for high availability and resilience across geographic locations. AWS data centers are designed with robust physical security controls and safeguards to help protect the underlying infrastructure. AWS customers have the ability to select the specific AWS Regions where their data and workloads will be located, based on their requirements. *Technological and Communications Infrastructure:* AWS provides a comprehensive set of security services (Amazon Virtual Private Cloud (VPC), AWS CloudTrail, Amazon GuardDuty, AWS WAF, AWS Shield) that customers can use to help secure their technological infrastructure. AWS operates and maintains the core networking and communications infrastructure that underpins its cloud services. AWS customers maintain control over network configurations, security groups, and other network-level security controls within their AWS environment. *Relationships with Third Parties:* AWS customers retain ownership and control of their data and resources on AWS, including when working with third-party software or service providers.	Not applicable.

Summary of requirements	AWS Considerations	Implementation
	AWS provides capabilities such as AWS Organizations and AWS Service Catalog to help customers manage access and permissions for third parties. Customers can use AWS Config and AWS CloudTrail to monitor third-party activities and resources within their AWS environment.	

Article 12. Minimum information security measures to be adopted by companies.

Summary of requirements	AWS Considerations	Implementation
1. Human Resources Security: **a)** Implement information security protocols applicable to the recruitment and incorporation of personnel, in the event of a change of role and termination of the employment relationship. **b)** Disciplinary processes in case of non-compliance with information security policies.	**Shared responsibility** AWS provides security services and features such as AWS Identity and Access Management (IAM), AWS CloudTrail, and AWS Security Hub to help customers implement identity and access management controls. AWS customers maintain full control over user identities, access, and permissions within their AWS environment. Customers are responsible for defining and enforcing their own information security protocols for personnel management, using the security capabilities offered by AWS. *Recruitment and Onboarding:* AWS customers are responsible for defining and implementing their own security training and onboarding procedures for personnel accessing the customer's AWS environment and resources. AWS has implemented a formal, documented security awareness and training policy that addresses the purpose, scope, roles, and responsibilities for all employees. AWS requires new hires to complete security awareness training prior to being granted access to AWS systems and data. *Change of Role:*	SEC 1 - Secure Operations SEC 2 - Authentication SEC 3 - Authorization and Access Control OPS 9 - Health of Operations

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for managing user access, permissions, and role changes within their own AWS environment using services such as AWS Identity and Access Management (IAM) and AWS Organizations. Customers can use AWS CloudTrail to audit and monitor changes to user permissions and access in their AWS environment. AWS has established procedures to warrant that employee access permissions are reviewed and updated when there are changes in roles or responsibilities. *Termination of Employment:* AWS customers are responsible for immediately revoking access and permissions for their own employees or third-party personnel upon termination of their relationship. Customers can use AWS CloudTrail and other monitoring services to verify that user access has been properly revoked across their AWS resources. AWS has defined processes to revoke access for employees upon termination of employment.	
2. Physical and logical access controls: **a)** Prevent unauthorized access to information, as well as to systems, equipment, and facilities through which it is processed, transmitted or stored, either in person or remotely.	**Shared responsibility** AWS provides the building blocks for physical and logical access controls, but AWS customers are responsible for designing, implementing, and operating the access management within their own AWS environment based on their security and compliance requirements. AWS customers maintain full control and ownership of their data and access to it. *Preventing unauthorized access:* AWS provides robust physical security controls at its data centers, including 24/7 staffed security, video surveillance, and multi-factor access control systems. AWS retains complete control over the physical access to the data centers.	SEC 2 - Authentication SEC 3 - Authorization and Access Control SEC 5 - Network Protection SEC 6 - Compute Protection

Summary of requirements	AWS Considerations	Implementation
b) Implement access management procedures, which should include access accounts with administrative privileges; ensuring a segregation of functions to reduce the risk of error or fraud, and following the principles of minimum privilege and need to know. **c)** Implement authentication processes to control access to information assets; in particular, in services provided to users through digital channels, authentication processes must meet the requirements established in Subchapter III of Chapter II of these Regulations.	Environments are logically segregated to prevent users and customers from accessing resources not assigned to them. AWS customers maintain full control over who has access to their data. AWS services providing virtualized operational environments to AWS customers such as Amazon Elastic Compute Cloud (Amazon EC2) check that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure through hypervisors and instance isolation. 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 is designed to erase every block of storage before making it available for use, which protects customer data from being unintentionally exposed. AWS customers can 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. AWS customers can learn more about logical separation on the Logical Separation on AWS whitepaper and the Infrastructure Security user guide. For logical access, AWS offers advanced identity and access management services such as AWS Identity and Access Management (IAM) that allow customers to control access to AWS resources. AWS customers can use AWS services to implement strong authentication, authorization, and access policies. *Access management procedures:*	

Summary of requirements	AWS Considerations	Implementation
	AWS customers maintain full control over user accounts and administrative privileges in their AWS environment. They can implement the principles of least privilege and segregation of duties using AWS Identity and Access Management (IAM). AWS has no visibility or control over the customer's user accounts and access management. This is the customer's responsibility within the shared responsibility model. *Authentication processes:* AWS 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 is designed to control user and programmatic access to AWS services and resources. AWS customers can apply granular policies, which assign permissions to a user, group, role, or resource and also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). AWS customers can use federation with their existing directory service. For workloads that require elevated access to AWS resources, IAM enables secure access through roles, instance profiles, identity federation, and temporary credentials. AWS provides various authentication options such as multi-factor authentication, federated access, and integration with customer's identity providers to help secure access to AWS services. AWS customers are responsible for configuring and managing the authentication mechanisms for their own applications and workloads running on AWS.	
3. Secure operations: **a)** Ensure and provide for the continuous operation of information processing, storage and transmission facilities.	**Customer responsibility**	REL 11 - Resiliency Implementation OPS 5 - Improve Production Flow OPS 6 - Mitigate Deployment Risk OPS 7 - Supporting a Workload OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
b) Maintain the operation of computer systems in accordance with previously established procedures. **c)** Control changes in the operating environment of systems, and keep development, test and production environments segregated.	AWS customers 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 architecture of their workloads 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 can meet specific geographic or regulatory requirements. *Continuous operation:* AWS manages the nearly continuous operation of the cloud infrastructure, and AWS customers are responsible for architecting resilient applications and implementing their own business continuity plans on top of the AWS infrastructure and services. AWS has designed its infrastructure to be highly available and resilient. The AWS global infrastructure is composed of Regions and Availability Zones (AZs), where each AZ is designed as an independent failure zone. AWS data centers are built with redundant power, cooling, and networking, and are designed to tolerate system or hardware failures with minimal customer impact. Automated processes move customer traffic away from impacted areas. AWS customers can use AWS services such as Amazon EC2, Amazon S3, Amazon RDS to architect highly available and fault-tolerant applications. Features such as multi-AZ deployments, auto-scaling, and data replication across AWS Regions/AZs help support nearly continuous operation. AWS provides customers the ability to implement their own robust business continuity and disaster recovery plans. AWS services such as AWS Backup, and AWS Outposts enable seamless data protection and migration. AWS has obtained ISO 22301 certification, demonstrating an effective business continuity management system to support customer resilience requirements. *Maintaining computer system operations:*	SEC 1 - Secure Operations

Summary of requirements	AWS Considerations	Implementation
	AWS manages and maintains the operational integrity of the underlying cloud infrastructure, and AWS customers are responsible for the operational procedures and practices for their own applications and workloads deployed on AWS. AWS manages the underlying infrastructure and services, verifying they are operated and maintained per industry best practices and standards. AWS has established comprehensive operational processes and procedures covering areas such as change management, incident response, problem management, and more. These are regularly tested and audited. AWS provides customers with a wide range of services and features to automate the management and maintenance of their own workloads and applications running on AWS. This includes services such as AWS Config, AWS Systems Manager, and AWS CloudFormation. The AWS Well-Architected Framework provides guidance to help customers design, deploy, and operate reliable, secure, efficient, and cost-effective systems in the cloud. AWS customers have visibility into the operational health and status of AWS services through tools such as the AWS Personal Health Dashboard and Amazon CloudWatch to monitor operational events. Customers are responsible for defining, implementing, and operating their own system administration procedures and practices within their AWS environments, including tasks such as: software updates, patch management, configuration management. AWS manages the change control and operational integrity of the underlying cloud infrastructure and AWS customers are responsible for implementing appropriate change management and environment segregation practices for their own applications and workloads deployed on AWS *Controlling changes in the operating environment:* AWS has established robust change management processes to control changes to the underlying cloud infrastructure. These include testing, approval, and rollback procedures. AWS provides customers the ability to implement their own change management processes and controls for their applications and workloads deployed on AWS. Customers can use AWS services such as AWS Config, AWS CloudTrail, and AWS Organizations to monitor, audit, and control changes within their own AWS environments. *Segregating environments:*	

Summary of requirements	AWS Considerations	Implementation
	AWS provides the ability to logically isolate development, test, and production environments through features such as Virtual Private Clouds (VPCs), security groups, and network ACLs. AWS customers have full control over creating separate AWS accounts, VPCs, subnets, and other resources to implement environment segregation that supports their requirements. AWS customers are responsible for implementing appropriate access controls, resource tagging, and monitoring to achieve proper segregation of environments within their AWS environments. AWS services such as AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy can help automate the deployment of application code between different environments.	
3. Secure operations (continued): **d)** Implement controls that ensure the integrity of transactions that are executed in computer services and systems. **e)** Restrict the installation of software on operating systems and prevent the exploitation of information security vulnerabilities.	**Shared responsibility** AWS enables customers to implement controls to achieve transaction integrity, but the specific design, implementation, and operation of those controls within the application logic is the customer's responsibility. *Ensuring transaction integrity:* AWS provides a variety of security services and features that customers can use to help protect the integrity of transactions: • **Data Encryption**: AWS offers encryption capabilities at rest and in transit to help protect data integrity. Customers can use AWS Key Management Service (AWS KMS) to manage their own encryption keys. • **Logging and Monitoring**: Services such as AWS CloudTrail, Amazon CloudWatch, and AWS Config are designed to provide logging and monitoring capabilities to track and audit changes to resources. • **Access Controls**: AWS Identity and Access Management (IAM) helps customers to implement fine-grained access controls and authorization policies to help protect access to resources. • **Integrity Validation**: Services such as Amazon S3 and Amazon EBS are designed to provide checksum validation to verify data integrity during storage and retrieval.	SEC 1 - Secure Operations SEC 3 - Authorization and Access Control SEC 6 - Compute Protection SEC 7 - Data Classification SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for implementing appropriate application-level controls and transaction validation logic within their own applications and systems running on AWS. AWS provides services such as Amazon API Gateway, AWS Lambda, and Amazon DynamoDB that customers can use to build highly secure, scalable and resilient transactional applications. AWS manages vulnerability detection and patching for the underlying cloud infrastructure and AWS customers are responsible for vulnerability management within their own applications and systems running on AWS infrastructure and services. *Restricting software installation:* AWS provides customers with complete control over the software and applications installed and running in their AWS environment. Customers can implement change management processes and access controls to govern what software can be installed on their AWS resources. Services such as AWS Systems Manager and AWS Config allow customers to track, audit and control software changes across their AWS environments. *Preventing vulnerability exploitation:* AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their instances and applications. Scans performed by customers must include customer IP addresses and not AWS endpoints. AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for the eight services listed in the AWS Customer Support Policy for Penetration Testing. 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 can establish 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.	

Summary of requirements	AWS Considerations	Implementation
	AWS takes security very seriously, and investigates all reported vulnerabilities. AWS 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 customers informed of progress as we investigate and mitigate reported security concerns. Customers will receive a non-automated response to their initial contact within 24 hours, confirming receipt of the reported vulnerability. Customers will 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 has a vulnerability management program that scans its infrastructure, identifies potential vulnerabilities, and applies security patches in a timely manner. AWS customers can use services such as Amazon Inspector and AWS Security Hub to conduct vulnerability assessments on their own workloads and applications running on AWS. AWS provides AWS customers the ability to receive security bulletins, notifications and advisories to stay informed about potential vulnerabilities. AWS makes available security configuration guidelines and recommendations to help customers harden their systems and applications. AWS customers are responsible for patching and updating any software they install and run on the AWS infrastructure and services, as well as securing their own applications and data.	
3. Secure operations (continued):	**Shared responsibility** AWS manages the infrastructure-level security and data protection and AWS customers are responsible for the data, applications, and workloads they run on AWS. AWS provides tools and services to enable effective backup, recovery, and incident response capabilities. *Malware response and recovery:*	OPS 7 - Supporting a Workload SEC 1 - Secure Operations SEC 6 - Compute Protection

Summary of requirements	AWS Considerations	Implementation
f) Have response and recovery protocols for malware incidents; generate and test backup copies of information, software and elements that facilitate their restoration. **g)** Define, implement and maintain secure configuration baselines for the use of devices and implementation of computer systems. **h)** Have a backup strategy and information restoration procedures in the face of possible incidents, of internal or external origin, that compromise the availability of information for operations and the productive environment of the data processing center.	AWS has established comprehensive incident response and security event management processes to detect, respond to, and recover from security incidents, including malware. AWS provides guidance and best practices to help customers develop effective security incident response plans. AWS customers can use security services such as Amazon GuardDuty, AWS Security Hub, and AWS CloudTrail to help detect and respond to potential malware incidents within their AWS environment. Customers are responsible for implementing their own malware protection, detection, and incident response capabilities for their applications and data on AWS. *Backup and restoration:* AWS offers a range of backup and data protection services such as Amazon S3, Amazon EBS, and AWS Backup to enable customers to create and manage backups of their data. AWS customers are responsible for implementing their own backup and restoration strategies, testing backup procedures, and ensuring the recoverability of their data and applications. AWS customers can configure backup schedules, retention policies, and encryption to help protect the availability and integrity of their data. AWS also provides services such as AWS Snow Family and AWS DataSync to facilitate secure data migration and transfer to and from the AWS Cloud. AWS customers are responsible for defining, implementing, and maintaining the secure configuration baselines for their own AWS resources and workloads. *Secure configuration baselines:* AWS provides customers with a wide range of services and tools to help define, implement, and maintain secure configurations across their AWS environment. • AWS Config allows customers to assess, audit, and evaluate the configurations of their AWS resources against desired baselines and industry standards. • AWS Security Hub aggregates security findings from various AWS services and third-party tools, providing a comprehensive view of the security posture and deviations from best practices. • AWS Systems Manager is designed to provide capabilities for patch management, software distribution, and configuration management, enabling customers to define and enforce secure configurations.	

Summary of requirements	AWS Considerations	Implementation
	AWS provides customers with prescriptive guidance and configuration templates through services such as AWS CloudFormation and the AWS Well-Architected Framework. *Implementation and maintenance:* AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within the 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 assets owned by AWS. The asset 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 our 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 understand the controls in place at AWS to maintain security and compliance in the cloud. AWS 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. AWS Artifact provides 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 AWS services to automate the deployment and enforcement of these secure configurations across their AWS environment. Ongoing monitoring, assessment, and remediation of deviations from the baseline configurations is the responsibility of the AWS customer. AWS provides customers the ability to delegate administrative access and permissions to enable appropriate separation of duties for configuration management.	
3. Secure operations (continued):	**Customer responsibility**	OPS 7 - Supporting a Workload OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
i) Have a backup strategy and information restoration procedures in the face of possible incidents, of internal or external origin, that compromise the availability of information for operations and the production environment of the data processing center.	AWS manages the availability and durability of the underlying storage services and AWS customers are responsible for defining their backup policies, schedules, retention periods, and restoration procedures based on their business requirements. AWS customers can design their backup architecture to meet their specific recovery time objectives (RTO) and recovery point objectives (RPO). *Backup strategy:* AWS provides a variety of services and features to enable customers to implement comprehensive backup and data protection strategies: • Amazon S3 for durable object storage with options for versioning, cross-region replication, and lifecycle policies. • Amazon EBS for block-level backup of Amazon EC2 instances. • AWS Backup for centralized backup management across various AWS services. • AWS Snow Family for offline data transfer and migration. • AWS DataSync for high-speed data transfer between on-premises and AWS. *Restoration procedures:* AWS customers are responsible for testing their backup and restoration procedures regularly to validate they can effectively recover from various failure scenarios. AWS provides guidance and best practices to help customers design resilient architectures and effective disaster recovery plans. AWS provides customers with the ability to restore data and applications from their backups stored in AWS. Services such as Amazon EC2, Amazon EBS, and AWS Backup enable customers to recover resources in the event of an incident.	
4. Secure communications:	**Shared responsibility** AWS manages the security of the underlying network infrastructure and AWS customers are responsible for configuring and securing their own network architectures, access controls, and monitoring within the AWS environment. *Secure communication networks:*	SEC 5 - Network Protection SEC 9 - Data Protection in Transit OPS 7 - Supporting a Workload OPS 10 - Workload and Operations Events REL 4 - Design Interactions to Prevent Failures

Summary of requirements	AWS Considerations	Implementation
a) Implement and maintain the security of communication networks in accordance with the information transmitted through it and the threats to which it is exposed. **b)** Ensure that communications networks and network services are managed and controlled to protect information.	AWS provides a variety of networking services and features that customers can use to secure their communication networks: • Amazon Virtual Private Cloud (VPC) for creating isolated, private networks within the AWS Cloud. • AWS Direct Connect for dedicated, private network connections between customer premises and AWS. • AWS VPN for establishing encrypted VPN tunnels between customer networks and AWS. • AWS WAF for web application firewall to help protect against common web issues. • AWS Shield for DDoS protection of customer applications. These services give AWS customers control over network access, help encrypt data in transit, and help protect against network-based threats such as DDoS attacks. AWS customers can also use AWS Security Groups and Network ACLs to implement granular network access controls and policies for traffic filtering. *Threat monitoring and response:* AWS has processes in place to identify, investigate and mitigate any network-based issues or anomalies that might impact the AWS infrastructure. AWS provides security monitoring and threat detection services such as Amazon GuardDuty and AWS Security Hub to help customers identify and respond to network-based security incidents. AWS customers can use AWS CloudTrail and Amazon CloudWatch to audit and monitor network activity within their AWS environments. *Network management and control:* AWS provides a comprehensive set of networking services and capabilities that AWS customers can use to manage and control their communication networks: • Amazon Virtual Private Cloud (VPC) for creating isolated, private networks within the AWS Cloud. • AWS Direct Connect for establishing dedicated, private network connections between customer premises and AWS. • Amazon Route 53 for secure and scalable Domain Name System (DNS) services.	REL 5 - Design Interactions to Mitigate Failures

Summary of requirements	AWS Considerations	Implementation
	• AWS PrivateLink for securely exposing services within a VPC to other VPCs or on-premises networks. • AWS Transit Gateway for centralizing network transit control and connectivity. These services help AWS customers set up, manage, and control their network architectures, access controls, routing, and connectivity within the AWS environment. *Network security and control:* AWS provides various security services and features to help customers protect and control their network communications: • AWS Security Groups and Network ACLs for granular network access control and traffic filtering. • AWS WAF (Web Application Firewall) for protecting against common web-based attacks. • AWS Shield for automatic protection against Distributed Denial of Service (DDoS) attacks. • AWS Network Firewall for managed, stateful firewall capabilities. AWS customers can use these services to implement network security controls, monitor network activity, and quickly respond to potential threats.	
4. Secure communications (continued): **c)** Segregate available information services, users, and systems in company networks.	**Customer responsibility** AWS provides networking, identity, and resource isolation capabilities and AWS customers are responsible for designing, implementing, and operating the appropriate segregation controls within their AWS environment based on their security and compliance requirements. *Segregating information services:* Amazon Virtual Private Cloud (VPC) allows customers to create logically isolated, private networks within AWS. AWS customers can further segment their VPCs using subnets, security groups, and network ACLs to isolate different applications, workloads, and information services. AWS PrivateLink enables secure communication between services within a VPC and other VPCs or on-premises resources, without exposing the services to the public internet. *Segregating users:*	SEC 5 - Network Protection SEC 9 - Data Protection in Transit OPS 7 - Supporting a Workload OPS 10 - Workload and Operations Events REL 4 - Design Interactions to Prevent Failures REL 5 - Design Interactions to Mitigate Failures

Summary of requirements	AWS Considerations	Implementation
	AWS Identity and Access Management (IAM) is designed to provide fine-grained access control, helping customers to segregate user access to specific AWS resources and services. AWS customers can implement the principle of least privilege and segregation of duties using IAM policies, roles, and multi-factor authentication. Integration with existing identity providers such as Active Directory enables seamless user access management and segregation. *Segregating systems:* AWS customers can use AWS Organizations to create multiple isolated AWS accounts, enabling strict segregation of environments. AWS customers can use container services such as Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS) to isolate and run applications in their own dedicated environments. AWS Config allows customers to monitor and audit the configurations of their AWS resources, to assess system segregation.	
4. Secure communications (continued): **d)** Implement secure protocols and security controls for the transfer of information, within the organization and with external parties.	**Customer responsibility** AWS customers are responsible for configuring the appropriate security controls, protocols, and access policies to help protect information transfer within their AWS environment and between AWS and external parties. *Secure protocols for information transfer:* AWS offers a range of secure protocol options for data transfer, both within the AWS environment and between AWS and external parties: • AWS PrivateLink for privately accessing AWS services and on-premises applications using private IP addresses, without exposing data to the public internet. • AWS Direct Connect for establishing dedicated, private network connections between customer premises and AWS. • AWS VPN for creating encrypted VPN tunnels between customer networks and AWS. • HTTPS/TLS for encrypting data in transit when accessing AWS services or customer applications. *Security controls for information transfer:*	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

Summary of requirements	AWS Considerations	Implementation
	AWS provides security controls to help customers protect the confidentiality, integrity, and availability of information during transfer: • AWS Key Management Service (AWS KMS) for creating and managing encryption keys used to help protect data in transit. • AWS CloudHSM for dedicated, hardware-based key storage and management. • AWS WAF (Web Application Firewall) for protecting against common web-based attacks that can compromise data in transit. • AWS Shield for automatic protection against Distributed Denial of Service (DDoS) attacks that can disrupt data transfer.	
4. Secure communications (continued): **e)** Ensure that remote access, the use of personal equipment on the company's network, mobile devices and the interconnection between own and third-party networks have controls in accordance with existing security threats.	**Customer responsibility** AWS provides the building blocks for secure remote access, bring your own device (BYOD), and network interconnections, but AWS customers are responsible for designing, implementing, and operating the appropriate security controls within their own AWS environment and applications. *Remote access controls:* AWS provides secure remote access capabilities through services such as AWS Direct Connect, AWS VPN, and AWS Client VPN. AWS customers can enforce multi-factor authentication, network access control, and other security policies for remote access to AWS resources. AWS Identity and Access Management (IAM) enables granular control over permissions and access for remote users. *Bring your own device (BYOD) and mobile device controls:* AWS supports secure access to resources from a variety of devices through features such as AWS Device Farm and Amazon WorkSpaces. AWS customers can use Mobile Device Management (MDM) solutions and integrate them with AWS to enforce security policies on mobile devices. The AWS IoT Core and AWS IoT Greengrass services enable secure connectivity and management of IoT devices, including mobile devices. *Network interconnection controls:*	SEC 2 - Authentication SEC 3 - Authorization and Access Control SEC 5 - Network Protection SEC 6 - Compute Protection

Summary of requirements	AWS Considerations	Implementation
	AWS PrivateLink allows customers to securely expose services within their VPC to other VPCs or on-premises networks, without exposing the service endpoints to the public internet. AWS Security Groups and Network ACLs provide granular network access control and traffic filtering capabilities. AWS Transit Gateway simplifies management and control of network connectivity between VPCs, on-premises networks, and AWS services.	
5. Acquisition, development, and maintenance of systems: **a)** Implement and maintain security in computer services and systems according to the information being processed and threats to which they are exposed.	**Shared responsibility** AWS is responsible for securing the cloud infrastructure and AWS customers are responsible for securing their own data, applications, and operating systems in the cloud. AWS Customers maintain full control over their content and are responsible for configuring access to AWS services and resources. *Security Features:* AWS offers industry-leading encryption features to help protect customer content in transit and at rest. Customers can choose to manage their own encryption keys using services such as AWS Key Management Service (AWS KMS). AWS provides access control, logging, and monitoring capabilities through services such as AWS Identity and Access Management (IAM), AWS CloudTrail, and Amazon CloudWatch. *Security Certifications:* AWS has obtained a wide range of security, compliance, and industry certifications, including ISO 27001, PCI DSS, and FedRAMP. Customers can use AWS Artifact to access audit reports and certifications to validate the security controls in place.	SEC 1 - Secure Operations SEC 3 - Authorization and Access Control SEC 2 - Authentication SEC 6 - Compute Protection OPS 5 - Improve Production Flow

Summary of requirements	AWS Considerations	Implementation
	AWS compliance programs help customers understand the controls in place at AWS to maintain security and data protection in the AWS Cloud. When systems are built on AWS, AWS and customers share compliance responsibilities. AWS computing environments are 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 has assurance programs that provide templates and control mappings to help customers asses the compliance of their environments running on AWS. For a full list of programs, see AWS Compliance Programs. Reports are available in AWS Artifact. *Incident Response:* AWS has a formal, documented incident response policy and program, with a three-phase approach for incident management. As part of the shared security responsibility model, security events monitoring must 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* will raise an incident and trigger the incident management process and any appropriate response actions necessary to mitigate the incident. 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	

Summary of requirements	AWS Considerations	Implementation
	AWS conducts incident response testing to validate the effectiveness of the AWS Incident Management plan. This testing provides coverage for the discovery of previously unknown defects and failure modes. 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 performed 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. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of AWS 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.	
5. Acquisition, development and maintenance of systems (continued): **b)** Ensure that information security practices are included in the planning, development, implementation, operation, support and deactivation of computer applications and systems.	**Customer responsibility** AWS provides security services and features to help AWS customers incorporate security throughout the entire application and system lifecycle. *Planning & Development:* AWS provides security and compliance whitepapers, architectural best practices, and design principles to help customers incorporate security during the planning and development phases. AWS customers can use AWS security services such as AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), and AWS CloudTrail to build security into their applications. *Implementation:*	OPS 5 - Improve Production Flow OPS 6 - Mitigate Deployment Risk OPS 7 - Supporting a Workload SEC 1 - Secure Operations

Summary of requirements	AWS Considerations	Implementation
	AWS CloudFormation allows customers to define and provision their AWS infrastructure in a secure, repeatable manner. AWS customers can use AWS Config to audit and evaluate the configurations of their AWS resources to verify they align with security best practices. *Operation & Support:* AWS provides monitoring and logging capabilities through services such as Amazon CloudWatch and AWS CloudTrail to help customers detect and respond to security events. AWS Security Hub aggregates security findings from various AWS services and third-party security tools to give customers a comprehensive view of their security and compliance posture. AWS Config Rules enables customers to monitor and remediate resource configurations for security and compliance requirements. *Deactivation or decommissioning:* AWS customers maintain full control over their content and can choose to securely delete their data when decommissioning resources. AWS provides the ability for customers to encrypt their data at rest and manage their own encryption keys, to support data protection during deactivation and decommissioning.	
5. Acquisition, development and maintenance of systems (continued): **c)** Limit access to modification of source program libraries and maintain strict change control.	**Customer responsibility** AWS provides several capabilities to help customers limit access and maintain change control for source program libraries: *Access Control:* AWS Identity and Access Management (IAM) allows customers to control who has access to modify source program libraries, down to the granular resource level. IAM supports multi-factor authentication, password policies, and fine-grained permissions to restrict access. AWS customers can use IAM roles and policies to limit which users or services have the ability to make changes to source program libraries. *Change Management:*	OPS 5 - Improve Production Flow OPS 6 - Mitigate Deployment Risk OPS 10 - Workload and Operations Events SEC 2 - Authentication SEC 3 - Authorization and Access Control

Summary of requirements	AWS Considerations	Implementation
	AWS CodeCommit is a fully-managed source control service that customers can use to store and version their source code. AWS CodeCommit is designed to provide branching, merging, and pull requests to enforce a structured change control process. AWS customers can integrate AWS CodeCommit with other AWS services such as AWS CodePipeline to implement their build, test, and deployment workflows. AWS Config can be used to track changes to AWS resources, including any changes made to source program libraries stored in AWS CodeCommit. *Auditing and Logging:* AWS CloudTrail logs all API calls made within the customer's AWS environment, including any changes made to source program libraries. AWS customers can use AWS CloudTrail to audit who made what changes, when, and from where. Amazon CloudWatch can be used to set up alarms and notifications for specific AWS CloudTrail events, enabling near real-time detection of unauthorized changes. Customers can limit access and maintain change control over their source program libraries in their AWS environments using AWS Identity and Access Management (IAM) for access control, AWS CodeCommit for change management, and AWS CloudTrail and Amazon CloudWatch for auditing and logging.	
5. Acquisition, development and maintenance of systems (continued): **d)** When the operating platform is changed, critical applications must be reviewed and tested to avoid adverse effects on their security.	**Customer responsibility** AWS offers change management, testing, and security capabilities to help customers review and test critical applications when the operating environment is changed: *Change Management Processes:* AWS Config can track changes to AWS resources, including changes to the underlying operating environment. Customers can use AWS Config Rules to monitor for changes and receive notifications when they occur. Customers can integrate AWS Config with other AWS services such as AWS CloudTrail and Amazon CloudWatch to build a comprehensive change management process. *Testing Environments:*	OPS 5 - Improve Production Flow OPS 6 - Mitigate Deployment Risk OPS 7 - Supporting a Workload

Summary of requirements	AWS Considerations	Implementation
	AWS provides services such as Amazon EC2, Amazon RDS, and AWS Lambda that allow customers to quickly provision and test applications in isolated environments. Customers can use AWS CloudFormation to define their application infrastructure as code, enabling them to easily replicate testing environments. AWS Outposts and Wavelength Zones allow customers to test applications in environments that mirror their production infrastructure. *Security Testing:* AWS Security Hub aggregates security findings from various AWS services and third-party security tools, giving customers a comprehensive view of their security posture. AWS Trusted Advisor is designed to provide security checks and recommendations to help customers identify and remediate risks. Customers can use AWS Marketplace to find and deploy third-party security testing tools within their AWS environment. *Rollback Capabilities:* AWS provides features such as Amazon Machine Images (AMIs) and AWS Backup that allow customers to quickly revert to a known good state if issues are identified during testing. Customers can use services such as Amazon EC2 Auto Scaling to automatically roll back to a previous version of their application if needed.	
5. Acquisition, development and maintenance of systems (continued): **e)** Ensure that technical, functional and information security tests are carried out on computer systems before they go into production.	**Customer responsibility** AWS provides several capabilities to help customers verify that technical, functional, and information security tests are conducted on computer systems before they go into production: *Testing Environments:* AWS offers a range of services that allow customers to quickly provision and test applications in isolated environments, such as Amazon EC2, Amazon RDS, and AWS Lambda. Customers can use AWS CloudFormation to define their application infrastructure as code, enabling them to easily replicate testing environments. AWS Outposts and Wavelength Zones allow customers to test applications in environments that mirror their production infrastructure. *Security Testing:*	OPS 5 - Improve Production Flow OPS 6 - Mitigate Deployment Risk OPS 7 - Supporting a Workload SEC 1 - Secure Operations

Summary of requirements	AWS Considerations	Implementation
	AWS Security Hub aggregates security findings from various AWS services and third-party security tools, giving customers a comprehensive view of their security posture. AWS Trusted Advisor is designed to provide security checks and recommendations to help customers identify and remediate risks. AWS customers can use AWS Marketplace to find and deploy third-party security testing tools within their AWS environment. *Automated Testing:* AWS provides services such as AWS CodeBuild and AWS CodePipeline that enable customers to implement continuous integration and continuous deployment (CI/CD) pipelines. These services allow customers to automate the use of technical, functional, and security tests as part of their application deployment workflows. AWS customers can integrate third-party testing tools and frameworks into their CI/CD pipelines to perform comprehensive testing before production deployment. *Validation and Approval:* AWS customers can use AWS Control Tower to establish a landing zone that enforces guardrails and best practices, including requirements for testing and approvals before production deployment. AWS Organizations and AWS Service Catalog can be used to centrally manage and control which AWS services and resources are available to developers, supporting alignment with corporate policies. Customers can implement custom approval workflows using AWS Lambda and Amazon Simple Notification Service (Amazon SNS) to require manual validation before production deployments. AWS customers can have comprehensive technical, functional, and information security tests conducted on computer systems before they go into production by using the AWS testing environments, security testing capabilities, and automated deployment tools.	
5. Acquisition, development and maintenance of systems (continued):	**Customer responsibility** AWS provides several capabilities to help customers implement and verify compliance with secure development practices for computer services and systems: *Secure Development Lifecycle:*	OPS 5 - Improve Production Flow OPS 7 - Supporting a Workload SEC 1 - Secure Operations

Summary of requirements	AWS Considerations	Implementation
f) Implement and verify compliance with procedures that include practices for the secure development of computer services and systems.	AWS provides guidance and best practices for incorporating security into the software development lifecycle, such as the AWS Well-Architected Framework and the AWS Security Maturity Model. These resources help AWS customers define and implement secure development processes, including secure coding practices, threat modeling, and security testing. *Development Environment Security:* AWS Identity and Access Management (IAM) allows AWS customers to control access and permissions for developers working on computer services and systems and AWS CodeBuild and AWS CodePipeline support secure software development practices by enabling customers to automate the build, test, and deployment of applications. AWS customers can integrate third-party security testing tools into their CI/CD pipelines to assess the security of their code. *Infrastructure as Code:* AWS CloudFormation enables customers to define their infrastructure as code, allowing them to version, review, and test infrastructure changes before deployment. AWS Config can monitor the configuration of AWS resources to validate they align with security best practices and compliance requirements. Customers can use AWS Service Catalog to centrally manage and provision pre-approved, secure infrastructure and application components. *Compliance and Certification:* AWS compliance programs help customers understand the controls in place at AWS to maintain security and data protection in the AWS Cloud. When systems are built on AWS, AWS and customers share compliance responsibilities. AWS computing environments are 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 has assurance programs that provide templates and control mappings to help customers asses the compliance of their environments running on AWS. For a full list of programs, see AWS Compliance Programs. Reports are available in AWS Artifact.	

Summary of requirements	AWS Considerations	Implementation
6. Cybersecurity incident management: **a)** Implement procedures for the management of cybersecurity incidents, as indicated in paragraph 8.2 of Article 8 of these Regulations; as well as, exchange information when appropriate, in accordance with Article 16 of these Regulations.	**Customer responsibility** Customers are responsible for establishing their own cybersecurity incident management team to implement the incident response plan. AWS provides incident response guidance, security services, and compliance resources, that customers can use to develop and implement comprehensive cybersecurity incident management procedures, establish an effective incident response team, and engage relevant third parties to effectively respond to threats and vulnerabilities. *Incident Response Plan:* AWS has a formal, documented incident response policy and program that follows a three-phase approach: Activation and Notification, Recovery, and Reconstitution. AWS provides guidance on developing an effective incident response plan in the AWS Security Incident Response Guide. Customers can use this guidance to establish their own comprehensive incident response plan and procedures. *Incident Response Team:* Customers are responsible for establishing their own cybersecurity incident management team to implement the incident response plan. AWS provides tools and services, such as Amazon CloudWatch, AWS CloudTrail, and Amazon GuardDuty, that can be used by the incident response team to detect, analyze, and respond to security incidents. AWS also offers professional services and training to help customers build and maintain their incident response capabilities. *Threat Intelligence and Vulnerability Management:* AWS Security Bulletins provide customers with information on the latest security news, vulnerabilities, and best practices. AWS Marketplace offers a variety of third-party security and threat intelligence tools that customers can integrate into their environments. AWS has a Vulnerability Reporting program that allows customers to report any security issues they identify in AWS services. *Third-Party Agreements:*	SEC 1 - Secure Operations OPS 9 - Health of Operations OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
	Customers are responsible for establishing agreements with relevant third parties, such as managed security service providers (MSSPs), to support their cybersecurity incident management and threat response capabilities. AWS provides a wide range of security and compliance-related documentation, including certifications and audit reports, that customers can use when evaluating and engaging third-party providers. In addition, the AWS Financial Services Enterprise Agreement contains terms and conditions to help financial services customers address their regulatory and legal requirements, including incident response and third-party management.	
6. Cybersecurity incident management (continued): **b)** Implement a methodology to classify cybersecurity incidents and provide response and recovery protocols. **c)** Have an information security operations service, including capabilities for detection and response, the monitoring of communications in the internal network and the degree of operation of the technological infrastructure. **d)** Have access to intelligence information on threats, vulnerabilities and incidents, as well as to knowledge bases of techniques and tactics used by threat actors.	**Customer responsibility** Customers are responsible for the implementation of their internal controls and policies and are responsible for reporting any cybersecurity incidents to the relevant regulatory authorities as required. AWS provides capabilities to help customers implement a methodology for classifying and responding to cybersecurity incidents, as well as supporting information security operations and internal reporting: *Incident Response:* AWS provides guidance on developing an effective incident response plan in the AWS Security Incident Response Guide. AWS has a formal, documented incident response policy and program, with a three-phase approach for incident management: Activation and Notification, Recovery, and Reconstitution. Customers can use AWS services such as Amazon CloudWatch, AWS CloudTrail, and Amazon GuardDuty to detect and respond to security events and incidents. *Security Operations:* AWS Security Hub aggregates security findings from various AWS services and third-party security tools, giving customers a comprehensive view of their security posture. Amazon GuardDuty is a threat detection service designed to monitor for unexpected activity and unauthorized behavior to help protect AWS accounts and workloads. AWS Config can be used to assess, audit, and evaluate the configurations of AWS resources to identify security issues.	*Security operations for detection and response:* OPS 9 - Health of Operations OPS 10 - Workload and Operations Events *Access to threat intelligence:* SEC 1 - Secure Operations *Internal and regulatory incident reporting:* OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
e) Implement internal reporting mechanisms for cybersecurity incidents, in accordance with the provisions of Article 8 of these Regulations, and to the Superintendency in accordance with Article 15 of these Regulations.	*Threat Intelligence:* AWS Security bulletins provide customers with information on the latest security news, vulnerabilities, and best practices. AWS Marketplace offers a variety of third-party security and threat intelligence tools that customers can integrate into their environments. AWS has a Vulnerability Reporting program that allows customers to report any security issues they identify in AWS services. *Incident Reporting:* AWS CloudTrail logs all API calls made within the customer's AWS environment, including any security-related events. Customers can use AWS CloudTrail to audit and report on security incidents, and integrate the logs with their own internal reporting mechanisms.	
6. Cybersecurity incident management (continued): **f)** Identify possible improvements for incorporation into the management of cybersecurity incidents, after their occurrence. **g)** Preserve evidence that facilitates forensic investigations after the occurrence of information security incidents.	**Shared responsibility** AWS provides capabilities to help customers identify improvements and preserve evidence after the occurrence of cybersecurity incidents. In addition, AWS provides guidance on developing an effective incident response plan in the AWS Security Incident Response Guide, which includes recommendations on post-incident activities and lessons learned. *Incident Review and Improvement Identification:* AWS has a formal, documented incident response policy and program, with a three-phase approach for incident management. As part of the shared security responsibility model, security events monitoring are 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* will raise an incident and trigger the incident management process and any appropriate response actions necessary to mitigate the incident. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase	*Continuous improvement of incident management:* OPS 9 - Health of Operations OPS 10 - Workload and Operations Events *Forensic evidence preservation:* OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
	2. Recovery Phase 3. Reconstitution Phase To verify the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides coverage for the discovery of previously unknown defects and failure modes. 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 performed 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. In addition, the AWS Personal Health Dashboard gives AWS customers a personalized view into the performance and availability of AWS services. It displays relevant and timely information to help customers manage events in progress, and is designed to provide proactive notification to help customers plan for scheduled activities. AWS Trusted Advisor is designed to provide security checks and recommendations to help customers identify and remediate risks, including those identified during incident response. *Forensic Investigation:* AWS CloudTrail records all API calls made within a customer's AWS environment, providing a detailed audit trail that can be used for forensic investigations. Amazon GuardDuty is designed to monitor for suspicious activity and can generate detailed security findings that can support forensic analysis. AWS Config can track changes to AWS resources, which can be relevant for understanding the context and timeline of a security incident.	

Summary of requirements	AWS Considerations	Implementation
	Data Preservation: AWS customers maintain full control over their data stored in AWS and can choose to encrypt it at rest and in transit, protecting it from unauthorized access. AWS provides the ability to take snapshots of resources such as Amazon EC2 instances and Amazon EBS volumes, which can be used to preserve evidence for forensic investigations. AWS Backup enables customers to create and manage backups of their AWS resources, and have their data readily available for forensic purposes.	
7. Physical and environmental security **a)** Implement controls to prevent unauthorized physical access, damage or interference to company information or processing facilities. **b)** Adopt measures to prevent loss, damage, theft or compromise of information assets and the interruption of operations, by protecting equipment and devices, and taking into account the environment in which they are used.	**Shared responsibility** AWS is responsible for the physical security and environmental controls of the underlying cloud infrastructure and AWS customers are responsible for securing their own data, applications, and operating systems running on AWS, as well as any on-premises equipment and devices they use. AWS provides physical and environmental security controls to help customers prevent unauthorized access, damage, and disruption to their information and infrastructure. AWS customers can protect their information assets and the continuity of their operations in the cloud using the physical and environmental security controls provided by AWS, along with the ability to integrate their own security solutions. *Physical Access Controls:* AWS data centers are highly secure facilities with multiple layers of physical access controls, including perimeter fencing, video surveillance, and 24/7 security personnel. Access to AWS data centers is restricted to authorized personnel only, with strict access control procedures in place. AWS data centers are designed to withstand adverse physical events, such as natural disasters and power outages. *Environmental Controls:*	*Prevent unauthorized physical access, damage, or interference:* SEC 6 - Compute Protection *Prevent loss, damage, theft, or compromise of information assets:* SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit OPS 7 - Supporting a Workload REL 11 - Resiliency Implementation

Summary of requirements	AWS Considerations	Implementation
	AWS data centers are equipped with redundant and diverse power, cooling, and networking capabilities to achieve high availability and prevent service disruptions. AWS utilizes robust environmental monitoring and automated response systems to detect and mitigate physical threats, such as fires, floods, and earthquakes. AWS data centers are located in lower-risk geographic regions to minimize exposure to environmental hazards. *Asset Protection:* AWS provides services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Elastic Block Store (Amazon EBS) to help customers securely store and manage their data and applications. AWS offers a range of encryption options, including customer-managed keys, to help protect data at rest and in transit. AWS services integrate with customer-owned security solutions, such as hardware security modules (HSMs), to provide an additional layer of protection for sensitive data. AWS 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. AWS 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.	
8. Cryptography **a)** Use cryptography to ensure the confidentiality, authenticity and integrity of information, both when the associated data is in storage and during transmission.	**Customer responsibility** AWS provides a comprehensive set of cryptography and key management services to help customers verify the confidentiality, authenticity, and integrity of their information, both at rest and in transit: *Data Encryption:*	*Use of cryptography:* SEC 2 - Authentication SEC 3 - Authorization and Access Control SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit *Cryptographic key management:* SEC 2 - Authentication

Summary of requirements	AWS Considerations	Implementation
b) Implement the necessary procedures to manage the lifecycle of the cryptographic keys to be used.	AWS offers encryption capabilities across a wide range of its services, including Amazon S3, Amazon EBS, Amazon RDS, and Amazon DynamoDB. AWS customers can choose to have AWS manage the encryption keys or bring their own keys using services such as AWS Key Management Service (AWS KMS) and AWS CloudHSM. AWS KMS allows customers to create and manage encryption keys, with options for customer-managed or AWS-managed keys. AWS CloudHSM is designed to provide AWS customers with dedicated, single-tenant, hardware-based key storage for their encryption keys. *Secure Communications:* AWS supports secure data transmission using industry-standard protocols, such as TLS, to help protect data in transit. Customers can use AWS Certificate Manager to provision, manage, and deploy public SSL/TLS certificates for use with their AWS services. AWS PrivateLink enables customers to privately access AWS services and their own applications, without exposing data to the public internet. *Key Management Lifecycle:* AWS Key Management Service (AWS KMS) is designed to provide comprehensive key management capabilities, including creation, rotation, and deletion of encryption keys. AWS customers can set custom key rotation policies and integrate key usage logging with AWS CloudTrail for auditing purposes. AWS CloudHSM allows customers to fully manage the lifecycle of their cryptographic keys within a FIPS 140-2 validated hardware security module. *Compliance and Standards:* AWS cryptographic services are designed to meet a wide range of compliance and industry standards, such as NIST, PCI DSS, HIPAA, and FedRAMP. Customers can use AWS Artifact to access audit reports and certifications that demonstrate the security and compliance of the cryptographic services provided by AWS.	SEC 8 - Data Protection at Rest OPS 7 - Supporting a Workload
9. Information Asset Management	**Customer responsibility**	*Identifying and managing information assets:*

Summary of requirements	AWS Considerations	Implementation
a) Identify information assets through an inventory, assign their custody, establish guidelines for their acceptable use and return them at the end of the agreement for which they were provided. **b)** Ensure that the level of protection and treatment of information is in accordance with its classification in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. **c)** Establish measures to prevent unauthorized disclosure, modification, deletion or destruction of information, in the use of removable devices.	AWS customers are responsible for the security and protection of their own data, applications, and information assets. AWS is responsible for the security of the underlying cloud infrastructure, including the physical security of the data centers and the security of the services that AWS customers use. AWS customers can identify, classify, and help protect their information assets, and verify they are accessed and used in accordance with their policies and legal requirements, by using security features and services in AWS. *Information Asset Inventory:* AWS Config is designed to help discover and inventory the AWS resources within a customer's environment, including the data stored and processed by those resources. AWS Service Catalog allows customers to create and manage catalogs of approved AWS resources, providing visibility and control over the services being used. AWS customers can use AWS tags and resource grouping to categorize and manage their information assets. *Information Classification and Protection:* AWS customers maintain full control over their content stored in AWS and are responsible for classifying and protecting their data based on its sensitivity and legal requirements. AWS provides a wide range of security features, such as encryption, access controls, and logging, to help customers protect their information assets. AWS customers can use services such as Amazon S3 Intelligent-Tiering and Amazon Glacier to automatically classify and store data based on access patterns and retention requirements. *Removable Media Protection:* AWS does not provide physical removable media devices to customers. All customer data is stored and processed within the AWS Cloud infrastructure. AWS customers can use AWS services such as Amazon EBS and Amazon EC2 to create, store, and manage their data in a secure, virtual environment without the need for physical removable media. AWS provides access control and encryption features to prevent unauthorized access, modification, or deletion of data, even in the event of a lost or stolen device.	SEC 7 - Data Classification OPS 7 - Supporting a Workload *Information classification and protection:* SEC 7 - Data Classification SEC 8 - Data Protection at Rest *Protecting against unauthorized access and modification:* SEC 3 - Authorization and Access Control SEC 6 - Compute Protection SEC 9 - Data Protection in Transit SEC 5 - Network Protection:

Article 13. Planned activities.

Summary of requirements	AWS Considerations	Implementation
Within the framework of the SGSI-C Strategic Plan, the company must maintain operational plans, at least for the following purposes: **a)** Identify information assets, classify them, analyze the threats and vulnerabilities associated with them, and take appropriate treatment measures. **b)** Subject the SGSI-C to periodic evaluations, reviews and tests to determine its effectiveness, through internal and external services, and depending on the level of complexity and threats to the associated information assets. Depending on the results obtained, incorporate the improvements or adopt corrective action. **c)** Address training needs, as appropriate to the roles and functions in the organization, in the area of information security and cybersecurity to ensure the effectiveness of the SGSI-C. **d)** Develop the cybersecurity program, in accordance with Subchapter II of Chapter II of these Regulations. **e)** Periodically review, and update when appropriate, the information security policies that are established to implement the requirements established in Article 12 of these Regulations.	**Customer responsibility** AWS manages the security of the cloud infrastructure, but AWS customers are responsible for the implementation and maintenance of their internal plans, controls, and policies. *Asset Management:* AWS customers are responsible for identifying, classifying, and managing their information assets on AWS. AWS provides services such as AWS Config, AWS Security Hub, and Amazon GuardDuty to help customers discover, classify, and monitor their resources and identify risks. In addition, AWS customers can use the AWS Well-Architected Framework to analyze threats and vulnerabilities, and implement appropriate security controls. *Evaluation and Testing:* AWS customers are responsible for periodically evaluating the effectiveness of their security controls and incident response plans. Customers can use compliance certifications and audit reports to validate the security of AWS. AWS provides AWS Artifact to give customers on-demand access to security and compliance reports from AWS, which can help with evaluations. *Training and Awareness:* AWS customers are responsible for training their employees on information security and cybersecurity best practices. AWS provides a wide range of training resources, including online courses, whitepapers, and hands-on labs, to help customers upskill their teams. *Cybersecurity Program:*	*Information asset management:* SEC 1 - Secure Operations SEC 7 - Data Classification SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit *Training and awareness:* SEC 1 - Secure Operations *Cybersecurity program:* SEC 1 - Secure Operations SEC 2 - Authentication SEC 3 - Authorization and Access Control SEC 5 - Network Protection SEC 6 - Compute Protection *Reviewing and updating security policies:* SEC 1 - Secure Operations

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for developing and implementing a comprehensive cybersecurity program. AWS provides services such as AWS Security Hub, Amazon GuardDuty, and AWS Config that can help customers build and automate their cybersecurity program. *Policy Review:* AWS customers are responsible for periodically reviewing and updating their information security policies. AWS provides documentation, whitepapers, and guidance to help customers align their policies with industry standards and best practices.	

SUBCHAPTER II CYBERSECURITY

Article 14. Cybersecurity program.

Summary of requirements	AWS Considerations	Implementation
14.1 Every company that has a presence in cyberspace must maintain, on a permanent basis, a cybersecurity program (PG-C) applicable to operations, processes and other associated information assets. **14.2** The PG-C must provide for a diagnosis and a plan to improve its cybersecurity capabilities, for which it must select an international reference framework on the subject, which allows at least the following: **a)** Identification of information assets. **b)** Protection against threats to information assets. **c)** Detection of cybersecurity incidents. **d)** Response with measures that reduce the impact of incidents. **e)** Recovery of technological capabilities or services that may be affected.	**Customer responsibility** *Identification of information assets:* AWS customers are responsible for identifying and classifying their information assets on AWS. AWS provides services such as AWS Config, Amazon GuardDuty, and AWS Security Hub to help customers discover, inventory, and classify their AWS resources. *Protection against threats:* AWS customers are responsible for protecting the security of their data, applications, and cloud environment. AWS is responsible for protecting the security of the cloud infrastructure. AWS provides a wide range of security services and features such as: AWS Identity and Access Management (IAM), encryption, and network security to help customers implement effective protective measures. *Detection of incidents:* AWS customers are responsible for monitoring their cloud environment and detecting security incidents. AWS provides services such as Amazon GuardDuty, AWS Security Hub, and AWS CloudTrail to help customers detect and investigate potential security issues. *Incident response:* AWS customers are responsible for developing and implementing incident response processes. AWS provides guidance and best practices to help customers build effective incident response capabilities. AWS also has its own incident management processes that customers can learn from. *Recovery and resilience:*	*Identification of information assets:* SEC 7 - Data Classification *Protection against threats to information assets:* SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit SEC 5 - Network Protection SEC 6 - Compute Protection *Detection of cybersecurity incidents:* SEC 10 - Incident Response OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events *Response with measures that reduce the impact of incidents:* SEC 10 - Incident Response REL 10 - Fault Isolation REL 11 - Resiliency Implementation *Recovery of technological capabilities or services affected:* OPS 7 - Supporting a Workload

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for architecting resilient and highly available systems on AWS. AWS provides services such as AWS Backup, AWS Snowball, and AWS Outposts to help customers implement data protection and disaster recovery strategies. The AWS infrastructure is designed for high availability and fault tolerance to support customer recovery objectives.	

Article 15. Report of significant cybersecurity incidents.

Summary of requirements	AWS Considerations	Implementation
15.1 The company must report to the Superintendency, as soon as it notices the occurrence of a cybersecurity incident that presents a significant verified or presumed adverse impact of: **a)** Loss or theft of company or customer information. **b)** Internal or external fraud. **c)** Negative impact on the company's image and reputation. **d)** Interruption of operations. **15.2** The company must carry out a forensic analysis to determine the causes of the incident and take measures for its management. The report resulting from this analysis must be available to the Superintendency, and must have executive content and also the corresponding technical detail. **15.3** The Superintendency, through a general rule, establishes the minimum content, format and additional protocols to be used in said report.	**Customer responsibility** AWS customers can use the security, monitoring, and logging capabilities of AWS to detect, investigate, and report on any significant security incidents as required by the Superintendency. AWS provides the building blocks, but the AWS customer is responsible for implementing the appropriate processes and procedures. *Incident Reporting:* AWS customers are responsible for monitoring their cloud environment, detecting security incidents, and reporting them to the Superintendency. AWS provides services such as Amazon GuardDuty, AWS Security Hub, and AWS CloudTrail to help customers detect and investigate potential security incidents. AWS customers can use these AWS services to gather the necessary information to report incidents to the Superintendency. *Forensic Analysis:* AWS customers are responsible for conducting forensic analysis to determine the causes of any significant security incidents. AWS provides features and services that can assist with forensic investigations: • AWS CloudTrail for logging API calls and user activity. • Amazon CloudWatch for centralized logging and monitoring. • Amazon S3 for secure storage of forensic data. • AWS Config for tracking resource changes. AWS customers can use these AWS capabilities to gather the technical details required for the incident report to the Superintendency. *Reporting Format and Protocols:* AWS customers are responsible for ensuring the incident report meets the content, format, and protocols specified by the Superintendency.	*Incident reporting and forensic analysis:* SEC 10 - Incident Response Supports the process of identifying, reporting, and responding to security incidents, and conducting investigation and analysis to determine the root cause of the incident. *Reporting to the Superintendency:* SEC 10 - Incident Response Supports the process of reporting the incident and forensic findings to the regulatory body, per their specified format and protocols. *SEC 10 can coordinate with these practices:* REL 10 - Fault Isolation REL 11 - Resiliency Implementation OPS 7 - Supporting a Workload OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events

Summary of requirements	AWS Considerations	Implementation
	AWS does not dictate the format or protocols, but can provide guidance to customers on best practices for incident response reporting. AWS customers can work with AWS Support or AWS Professional Services to understand how to use AWS services and features to collect the necessary information for the incident report.	

Article 16. Cybersecurity Information Exchange.

Summary of requirements	AWS Considerations	Implementation
16.1 The company must make the necessary arrangements to have information that allows it to take timely action in the face of cybersecurity threats and for the treatment of vulnerabilities. **16.2** When exchanging information related to cybersecurity, the company may sign agreements with other companies in the sector or with third parties that are relevant, on a bipartisan, collective or trade union basis, for which they will define the relevant criteria. **16.3** By means of a general rule, the Superintendency may establish specific requirements to be incorporated into the exchange of cybersecurity information.	**Customer responsibility** AWS customers have full ownership of their threat and vulnerability management processes, while using the security services and features provided by AWS. *Timely Action against Cybersecurity Threats:* AWS customers are responsible for implementing processes and procedures to detect, analyze, and respond to cybersecurity threats in a timely manner. AWS provides several services that can support customers: • Amazon GuardDuty for threat monitoring and detection. • AWS Security Hub for aggregating and prioritizing security findings from multiple sources. • AWS Config for tracking resource changes that can indicate threats. • AWS CloudTrail for logging API activity that might reveal suspicious behavior. AWS customers can use these AWS services, along with their own security operations, to gain visibility and respond quickly to cybersecurity threats. *Vulnerability Management:* AWS customers are responsible for identifying, assessing, and remediating vulnerabilities in their cloud environment. AWS supports customers with security bulletins to inform of vulnerabilities in AWS services, making security and compliance reports (SOC, ISO) available to customers to assess the AWS control environment, and offering services such as AWS Systems Manager and Amazon Inspector designed to help customers scan for and remediate vulnerabilities. AWS customers can use these AWS capabilities as part of their vulnerability management program. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their instances and applications. Scans performed by customers must include customer IP addresses and not AWS endpoints. AWS customers	SEC 1 - Secure Operations Supports establishing secure operations, including processes for monitoring and responding to security threats. Also supports vulnerability management, including processes for identifying, assessing, and remediating vulnerabilities in a timely manner. The specific requirements from the Superintendency can be incorporated into these processes. *Additional relevant practices:* SEC 5 - Network Protection SEC 6 - Compute Protection These practices help support the underlying infrastructure against threats.

can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for the eight services listed in the AWS Customer Support Policy for Penetration Testing.

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 can establish 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.

AWS takes security very seriously, and investigates all reported vulnerabilities. AWS 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 customers informed of progress as we investigate and mitigate reported security concerns. AWS customers will receive a non-automated response to their initial contact within 24 hours, confirming receipt of the reported vulnerability. AWS customers will 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.

Information Sharing Agreements:

AWS customers are responsible for establishing any necessary information sharing agreements with other companies or third parties.

AWS does not directly participate in or dictate the terms of these information sharing arrangements. However, AWS can provide guidance on best practices for secure information exchange, using services such as AWS Key Management Service (AWS KMS) for encryption, and AWS CloudTrail for logging.

	The Superintendency might establish specific requirements for the exchange of cybersecurity information. In such cases, AWS can work with customers to understand how AWS services and capabilities can support compliance with those requirements.

SUBCHAPTER III AUTHENTICATION

Article 17. Authentication processes.

Summary of requirements	AWS Considerations	Implementation
17.1 The company must implement authentication processes, in accordance with the definition established in these Regulations; to control access to the services it provides to its users through digital channels, before which it must formally evaluate and take action on: **a)** The authentication factor(s) that will be required. **b)** Current cryptographic standards, based on software or hardware, and their expected confidentiality or integrity features. **c)** Terms and conditions under which it will be mandatory to require the user to re-authenticate, including and not limited to cases of inactivity or prolonged use of systems.	**Customer responsibility** AWS customers are responsible for defining and implementing their authentication policies and security controls and can use the security capabilities provided by AWS services such as AWS Identity and Access Management (IAM), AWS CloudTrail, and cryptography. *Authentication Factors:* AWS customers can define the appropriate authentication factors based on their risk assessment and security requirements. AWS Identity and Access Management (IAM) allows customers to control access to AWS resources using multi-factor authentication (MFA) mechanisms such as hardware or virtual MFA devices. *Cryptographic Standards:* AWS provides customers the ability to use industry-standard cryptographic algorithms and protocols for authentication, such as TLS, HTTPS, and FIPS 140-2 validated cryptography. AWS customers can configure their AWS resources to enforce the use of these strong cryptographic standards. *Re-authentication Requirements:* AWS customers can configure AWS Identity and Access Management (IAM) to enforce re-authentication requirements based on parameters such as session duration, user inactivity, or other custom conditions. AWS provides the flexibility for customers to define their own re-authentication policies to meet their security needs. *Security Controls:*	*Authentication factors:* SEC 2 - Authentication Use appropriate authentication mechanisms, including factors such as passwords, biometrics, and multi-factor authentication. *Cryptographic standards:* SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit Support current cryptographic standards to achieve confidentiality and integrity of data. *Re-authentication requirements:* SEC 3 - Authorization and Access Control This practice supports defining policies around session management and re-authentication, because of inactivity or prolonged use. *Security controls for authentication:* SEC 2 - Authentication SEC 3 - Authorization and Access Control SEC 5 - Network Protection These practices cover baseline controls such as limiting failed attempts, preventing attacks, and secure message handling. *Audit log guidelines:*

Summary of requirements	AWS Considerations	Implementation
d) Baseline of information security controls required to prevent threats to the authentication process, including, and not restricted to, the limited number of failed authentication attempts, the prevention of interception attacks and message manipulation. **e)** Guidelines for the retention of audit records for the detection of known threats and information security events.	AWS Identity and Access Management (IAM) is designed to provide controls such as limiting failed authentication attempts, protecting against credential theft, and end-to-end encryption of authentication requests. AWS customers can use these capabilities to implement security controls around their authentication processes. *Audit Logging:* AWS CloudTrail is designed to provide comprehensive logging of API calls and user activities, including authentication events. AWS customers can use AWS CloudTrail, along with other AWS monitoring services, to retain audit records and detect security threats related to authentication.	SEC 1 - Secure Operations This practice includes guidelines for logging and monitoring security-relevant events for detection and investigation. *Additional relevant practices:* SEC 6 - Compute Protection REL 6 - Monitor Performance These practices support the security and availability of the authentication and authorization systems.
17.2 Authentication processes must be re-evaluated whenever the technology used for their implementation is no longer supported by the manufacturer, or after the discovery of new vulnerabilities that may expose them.	**Customer responsibility** AWS customers are responsible for monitoring their authentication technologies, assessing risks, and initiating re-evaluation and remediation as required. AWS provides tools and services to facilitate these activities, but the responsibility lies with the AWS customer *Monitoring for Technological Obsolescence:* AWS customers are responsible for monitoring the support status and vulnerability landscape of the authentication technologies they have implemented. AWS does not directly manage the lifecycle of customer-controlled authentication mechanisms. However, AWS can provide guidance on industry best practices for monitoring technology obsolescence. *Responding to New Vulnerabilities:* When new vulnerabilities are discovered in authentication technologies used by AWS customers, it is the AWS customer's responsibility to assess the impact and take appropriate remediation actions.	*Monitoring for technological obsolescence:* SEC 2 - Authentication This practice covers the overall management of authentication mechanisms, including reviewing and updating them. *Re-evaluate authentication processes when the underlying technology is no longer supported by the manufacturer:* Follow SEC 1 - Secure Operations practices around vulnerability and patch management. *New vulnerabilities might expose the authentication process:* Follow SEC 1 - Secure Operations practices for threat and vulnerability management. *Additional relevant practices:* SEC 3 - Authorization and Access Control

Summary of requirements	AWS Considerations	Implementation
	AWS provides services such as Amazon Inspector and AWS Systems Manager to help customers scan for and remediate vulnerabilities in their environments. AWS proactively communicates security bulletins and advisories to customers when vulnerabilities are discovered in AWS services. AWS customers can use this information to assess potential knock-on effects on their own authentication implementations. *Re-evaluation of Authentication Processes:* AWS customers must have a defined process to re-evaluate their authentication mechanisms when necessary: • Review support status of underlying technologies. • Assess impact of newly discovered vulnerabilities. • Update authentication policies, controls, and implementation. AWS can provide architectural guidance and recommendations to assist customers in updating their authentication processes. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring, and intrusion detection for their instances and applications. Scans performed by customers must include customer IP addresses and not AWS endpoints. AWS customers can carry out security assessments or penetration tests against their AWS infrastructure without prior approval for the eight services listed in the AWS Customer Support Policy for Penetration Testing. 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 can establish 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.	Covers the broader access control policies and mechanisms that work in conjunction with the authentication processes. SEC 5 - Network Protection Network-level security controls that help protect the authentication infrastructure. SEC 10 - Incident Response Identification, response, and remediation of incidents related to authentication vulnerabilities or exposures.

Summary of requirements	AWS Considerations	Implementation
	AWS takes security very seriously, and investigates all reported vulnerabilities. AWS 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 customers informed of progress as we investigate and mitigate reported security concerns. AWS customers will receive a non-automated response to their initial contact within 24 hours, confirming receipt of the reported vulnerability. AWS customers will 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.	
17.3 The company must maintain and protect detailed records of what was done during each user enrollment, authentication attempt and each operation that requires prior authentication.	**Customer responsibility** AWS customers can use the logging, encryption, access control, and monitoring capabilities available on AWS to maintain a secure, tamper-evident record of user authentication activities. AWS provides the building blocks, but the specific implementation is the AWS customer's responsibility. *Logging User Activities:* AWS CloudTrail is a service that AWS customers can use to log API calls and user activities, including user authentication events. AWS customers can configure AWS CloudTrail to capture detailed records of user enrollment, authentication attempts, and other security-relevant actions. The logged data can be stored in secure locations such as Amazon S3 buckets and monitored using other AWS services such as Amazon CloudWatch. *Protecting Authentication Records:*	SEC 1 - Secure Operations Establish secure logging and monitoring capabilities to record security-relevant events, including detailed logs of user enrollment, authentication attempts, and other sensitive operations. SEC 2 - Authentication Logs capture information about the authentication events and factors used. SEC 3 - Authorization and Access Control Logs also record the authorized actions taken by users after authentication. SEC 8 - Data Protection at Rest

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for ensuring the integrity and confidentiality of the authentication records they maintain. AWS provides services and features to help customers protect these records: • Server-side encryption options for data at rest in Amazon S3, AWS CloudTrail, and other services. • Client-side encryption using AWS Key Management Service (AWS KMS). • Fine-grained access controls using IAM policies. • VPC flow logs and AWS Config for monitoring changes to data stores. *Monitoring and Alerting:* AWS customers can use services such as Amazon GuardDuty, AWS Security Hub, and Amazon CloudWatch to monitor for suspicious activities related to authentication records. Automated alerting and investigation capabilities in these services can help customers detect and respond to potential tampering or unauthorized access. *Archiving and Retention:* AWS customers are responsible for defining appropriate retention policies for their authentication records based on their compliance requirements. AWS provides storage services such as Amazon S3 and Amazon Glacier that AWS customers can use for long-term archiving and preservation of these records.	User activity logs need to be stored securely and protected from unauthorized access or tampering. SEC 9 - Data Protection in Transit If the logs are transferred to a centralized logging service, the transport must be secured. SEC 10 - Incident Response Logging and monitoring capabilities can feed into the customer's incident response process, enabling investigation and forensics in the event of a security incident. REL 6 - Monitor Performance The logging infrastructure needs to be monitored and maintained for reliability and availability.
17.4 The company must have tools and procedures to implement transaction monitoring that allows measures to be taken to reduce the possibility of fraudulent operations, incorporating already known fraud scenarios, and the theft or compromise of the elements used for authentication.	**Customer responsibility** AWS customers are responsible for their transaction monitoring and fraud prevention strategy and can use the security capabilities of AWS to help protect underlying authentication elements and data. *Transaction Monitoring Tools:* AWS provides services that customers can use for transaction monitoring and fraud detection: • Amazon GuardDuty for monitoring and threat detection. • Amazon Fraud Detector for building customized fraud detection models. • Amazon Comprehend for natural language processing to identify suspicious activities.	SEC 2 - Authentication Authentication processes can include mechanisms to detect and prevent the theft or compromise of authentication elements. SEC 3 - Authorization and Access Control Access controls and authorization policies can help limit the ability to perform fraudulent transactions. SEC 5 - Network Protection

Summary of requirements	AWS Considerations	Implementation
	• Amazon Athena and Amazon Redshift for querying and analyzing transaction data. *Incorporating Fraud Scenarios:* AWS customers are responsible for defining the specific fraud scenarios and patterns they want to detect. AWS provides analytical capabilities, but AWS customers must configure the appropriate rules, models, and detection logic based on their domain knowledge and historical fraud patterns. *Protecting Authentication Elements:* AWS provides security controls to help protect the integrity of authentication elements: • Amazon Identity and Access Management (IAM) access and permissions to authentication credentials. • AWS Key Management Service (AWS KMS) secure storage and management of cryptographic keys. • AWS CloudTrail log API calls related to authentication. AWS customers can use these AWS services to implement security best practices around their authentication mechanisms. *Incident Response and Reporting:* When fraudulent activities are detected, AWS customers are responsible for investigating, containing, and reporting the incidents following the AWS customer's policies and regulatory requirements. AWS can provide forensic data from its logging and monitoring services to assist AWS customers in their investigations.	Securing the network infrastructure can prevent unauthorized access that might enable fraud. SEC 6 - Compute Protection Help protect the compute resources used for transaction processing. SEC 10 - Incident Response The customer's incident management process can respond to and investigate fraudulent activities. OPS 8 - Health of a Workload Monitoring the health and behavior of the transaction processing systems can help detect anomalous activities. OPS 9 - Health of Operations Broader monitoring of the overall operational health can also surface potential fraud indicators. OPS 10 - Workload and Operations Events Logging and analyzing relevant events and metrics can help identify known fraud scenarios. REL 6 - Monitor Performance Monitoring the performance of the transaction systems can complement the fraud detection capabilities.

Article 18. User enrollment in services provided by digital channels.

Summary of requirements	AWS Considerations	Implementation
18.1 The enrollment of a user in a digital channel requires at least: **a)** Verify the identity of the user and take the necessary measures to reduce the possibility of impersonation, including the use of two biometric factors or the use of two independent factors from different categories, according to paragraph j) of article 2 of these Regulations, except in the case of insurance products included in the simplified customer due diligence regime, as established in article 31 of the Regulations for the Management of Money Laundering and Terrorism Financing Risks, approved by Regulation S.B.S. 2660-2015 and its amendments, in which case the use of a single biometric factor is permitted. **b)** Generate the credentials and assign them to the user.	**Customer responsibility** AWS customers are responsible for implementing a user identity verification process and enforcing multi-factor authentication (MFA) for their digital channels. AWS provides the necessary building blocks through services such as AWS Identity and Access Management (IAM), but the specific enrollment and authentication requirements are the AWS customer's responsibility. *Verifying User Identity:* AWS customers are responsible for implementing robust identity verification processes for user enrollment in digital channels. AWS does not directly perform user identity verification, because this is a customer-specific process. However, AWS can provide guidance and recommendations on industry best practices for identity proofing. *Implementing Multi-Factor Authentication:* AWS supports a variety of MFA options, including TOTP-based, U2F security keys, and hardware security tokens. AWS Identity and Access Management (IAM) is designed to provide customers the ability to enforce MFA for access to AWS resources and services. AWS customers can configure IAM to require users to provide two or more authentication factors, such as a password and a hardware or virtual MFA device, during the login process. *Reducing Impersonation Risks:* AWS customers can reduce the risk of user impersonation and unauthorized access by using MFA. AWS customers can also integrate IAM with their own identity providers using federation or single sign-on (SSO) capabilities. *Generate the credentials and assign them to the user*	*Verify user identity and reduce impersonation risk:* SEC 2 - Authentication This practice supports implementing strong authentication mechanisms, including the use of multiple factors from different categories. For example, something you know, something you have, and something you are. *Generate and assign user credentials:* SEC 2 - Authentication This practice supports the secure generation, assignment, and management of user credentials. For example, passwords, keys, and certificates. *Additional considerations:* SEC 3 - Authorization and Access Control Customers can have access controls in place based on the verified user identity. SEC 1 - Secure Operations Customers can incorporate secure enrollment and credential management processes into their security operations. SEC 10 - Incident Response

Summary of requirements	AWS Considerations	Implementation
	AWS customers can use the credential management capabilities of IAM to generate, assign, and secure user credentials as part of their digital channel enrollment process. AWS provides the underlying services, but the specific implementation of credential management policies and procedures is the AWS customer's responsibility. *Credential Generation:* AWS Identity and Access Management (IAM) is designed to provide customers the ability to create and manage user credentials, such as: • IAM user accounts with associated username and password. • IAM access keys for programmatic access. • Multi-factor authentication (MFA) devices, including hardware and virtual tokens. *Credential Assignment:* After the user's identity has been verified, AWS customers can use IAM to create the necessary credentials and assign them to the user. IAM allows AWS customers to define granular access permissions and policies to control what actions the user can perform with their credentials. AWS customers can also use IAM roles, federation, and single sign-on (SSO) to manage user access and credentials. *Credential Security:* AWS provides security features to help customers protect user credentials: • Password policies to enforce strong password requirements. • MFA enforcement to add an extra layer of authentication. • Encryption of credentials at rest and in transit. • Detailed logging and monitoring of credential usage through AWS CloudTrail. *Credential Lifecycle Management:* AWS customers are responsible for implementing processes to manage the entire credential lifecycle, including: • Secure credential provisioning and distribution. • Periodic rotation or replacement of credentials. • Prompt revocation of credentials upon user termination or role changes.	Customers can enable incident response capabilities to detect and mitigate potential impersonation attempts or credential compromises. SEC 8 - Data Protection at Rest Storing user credentials and enrollment data. SEC 9 - Data Protection in Transit Protecting the enrollment process and credential assignments during transmission.

Summary of requirements	AWS Considerations	Implementation
	AWS Identity and Access Management (IAM) is designed to provide controls, such as password policies, to help customers strengthen their authentication mechanisms and help protect against credential-based attacks.	
18.2 The company must manage the lifecycle of the credentials it generates and assigns to its users, for which it must provide procedures for their activation, suspension, replacement, renewal and revocation; as well as, where appropriate, to ensure their confidentiality and integrity.	**Customer responsibility** AWS customers are responsible for defining and implementing the appropriate credential lifecycle management procedures. AWS customers can use the credential management capabilities provided by AWS Identity and Access Management (IAM) and related services. *Credential Lifecycle Management:* AWS customers are responsible for defining and implementing procedures to manage the full lifecycle of user credentials, including: • Activation - Enabling new credentials for user access. • Suspension - Temporarily disabling access via credentials. • Replacement - Issuing new credentials to replace existing ones. • Renewal - Updating expired or expiring credentials. • Revocation: Permanently disabling and removing credentials. AWS Identity and Access Management (IAM) is designed to provide customers the necessary capabilities to support these credential lifecycle management processes: *Activation and Provisioning:* AWS customers can use IAM to create new user accounts and generate initial credentials; for example, passwords and access keys. IAM allows AWS customers to define policies to automatically enforce password complexity, expiration, and other security requirements. *Suspension and Revocation:* AWS customers can use IAM to suspend or revoke user credentials, either individually or in bulk. IAM is designed to provide access control features to enable prompt revocation of credentials upon user termination or role changes. *Replacement and Renewal:*	*Credential lifecycle management:* SEC 2 - Authentication This practice covers the lifecycle of user credentials, including: Activation, Suspension, Replacement, Renewal, and Revocation SEC 8 - Data Protection at Rest Securely storing credential data to maintain confidentiality. SEC 9 - Data Protection in Transit Protecting the confidentiality and integrity of credentials during transmission. *Additional considerations:* SEC 3 - Authorization and Access Control Tying the credential lifecycle events to the appropriate access control policies. SEC 1 - Secure Operations Incorporating credential lifecycle management into the overall security operations. SEC 10 - Incident Response Enabling revocation of credentials in response to security incidents.

Summary of requirements	AWS Considerations	Implementation
	AWS customers can use IAM to rotate or replace user credentials, such as updating passwords or regenerating access keys. IAM supports automatic expiration and renewal of credentials based on defined policies. *Confidentiality and Integrity:* AWS provides encryption options to help protect the confidentiality of credentials at rest and in transit. IAM integrates with AWS Key Management Service (AWS KMS) to enable customer-managed encryption keys. AWS CloudTrail is designed to provide detailed logging of credential usage to maintain integrity and enable auditing.	

Article 19. Strong authentication for digital channel operations.

Summary of requirements	AWS Considerations	Implementation
Strong authentication is required for those actions that may lead to fraudulent transactions or other abuse of the service to the detriment of the customer, such as transactions through a digital channel that involve payments or transfer of funds to third parties, registration of a trusted beneficiary, modification of the contracted savings/investment insurance products, the contracting of a product or service, modification of limits and conditions, for which it is necessary to: **a)** Use a combination of authentication factors, according to paragraph j) of Article 2 of these Regulations that, at least, correspond to two different categories and that are independent of each other.	**Customer responsibility** AWS customers are responsible for implementing strong authentication on their digital channels. AWS provides capabilities for multi-factor authentication through IAM, and enables customers to extend and integrate their own biometric authentication solutions. *Authentication factor - Something the User Knows:* AWS Identity and Access Management (IAM) allows AWS customers to implement password-based authentication, where users provide a password or passphrase as the knowledge-based factor. IAM supports various password policy configurations to enforce strong, complex passwords. *Authentication factor - Something the User Has:* IAM enables the use of hardware or virtual Multi-Factor Authentication (MFA) devices, such as security keys or authenticator apps, as the possession-based factor. AWS customers can require users to provide a one-time code from their MFA device in addition to their password during the authentication process. *Authentication factor - Biometric Information:* AWS does not directly integrate biometric authentication mechanisms, because this is typically implemented at the application level by the AWS customer. However, AWS services such as Amazon Cognito are designed to provide integration points where AWS customers can incorporate their own biometric authentication solutions, such as fingerprint or facial recognition. *Independence of Factors:* The three factors (knowledge, possession, biometric) are completely independent of each other in the AWS environment. AWS customers have full control over how they configure and integrate the different authentication factors, so they can prevent the factors from being related or reliant on each other.	*Multi-factor authentication (MFA):* SEC 2 - Authentication This practice supports the use of MFA, which requires users to present two or more authentication factors from different categories. *Key aspects to consider:* Use at least two independent factors from different categories that do not rely on the same underlying credential or device to prevent unauthorized access. Factors must be independent of each other. They must not be connected or easily linked back to the same user or device to further reduce the risk of impersonation or credential compromise. *Additional relevant practices:* SEC 3 - Authorization and Access Control Integrating the MFA requirements into the access control policies. SEC 1 - Secure Operations Verify that the MFA mechanisms are properly configured, maintained, and monitored. SEC 10 - Incident Response Enabling quick revocation of MFA factors in response to security incidents.

Summary of requirements	AWS Considerations	Implementation
b) Implement a control against man-in-the-middle attacks, which may include generating a unique authentication code using cryptographic methods, based on the specific data of each operation, which must be used only once. **c)** When the operation is successful, report the transaction data to the user.	**Customer responsibility** AWS customers are responsible for the generation of authentication codes and can use the cryptographic capabilities of AWS Key Management Service (AWS KMS) and AWS CloudHSM to generate secure, one-time authentication codes, and then integrate these codes into their application-level authentication flows. AWS customers are also responsible for implementing the user-facing transaction reporting functionality using other AWS services. *Generating One-Time Authentication Codes:* AWS provides several services and features that can help AWS customers generate one-time authentication codes using cryptographic methods: • AWS Key Management Service (AWS KMS) enables customers to create and manage their own cryptographic keys, which can be used to generate one-time codes. • AWS CloudHSM is designed to provide customers with dedicated, single-tenant hardware security modules (HSMs) to securely generate and store cryptographic keys for one-time codes. AWS customers can also integrate their own cryptographic libraries and algorithms with AWS services to generate unique, one-time authentication codes for each transaction. *Using One-Time Codes for Authentication:* AWS customers can integrate those one-time authentication codes generated using AWS services into their application-level authentication flows. For example, AWS customers can prompt users to enter the one-time code alongside other credentials such as username and password to complete the authentication process for a specific transaction. AWS Identity and Access Management (IAM) is designed to provide flexibility for AWS customers to incorporate one-time codes as an additional authentication factor. *Reporting Successful Transaction Data:*	*One-time authentication codes:* SEC 2 - Authentication This practice supports the use of one-time authentication codes generated using cryptographic methods. *Reporting transaction data:* SEC 9 - Data Protection in Transit This practice supports protecting the confidentiality and integrity of the data during transmission. *Additional considerations:* SEC 3 - Authorization and Access Control Integrating the one-time code validation into the overall access control policies. SEC 8 - Data Protection at Rest Securely storing any relevant transaction data. SEC 10 - Incident Response Enabling incident response capabilities to quickly detect and mitigate any issues with the one-time codes or transaction data. OPS 8 - Health of a Workload Monitoring the performance and behavior of the authentication and transaction reporting systems.

Summary of requirements	AWS Considerations	Implementation
	AWS customers are responsible for reporting the relevant transaction data back to the user after a successful transaction. AWS does not directly handle the user-facing transaction reporting, because this is a functionality at the application level. AWS provides a range of services that AWS customers can use to store, process, and present the transaction data to users, such as Amazon S3, Amazon DynamoDB, Amazon Redshift, and Amazon QuickSight.	

Article 20. Exemptions from reinforced authentication for digital channel operations.

Summary of requirements	AWS Considerations	Implementation
20.1 The following operations carried out through digital channels are exempt from the requirement for strong authentication indicated in Article 19 of these Regulations, except for the provision indicated in its paragraph (c) (notification of transaction data to user when the transaction is successful): **a)** Payment transactions, periodic payments or transfers to a beneficiary previously registered by the user as a trusted beneficiary, as the usual recipient of such transactions. **b)** Payment transactions, periodic payments or transfers to accounts where the customer and the beneficiary are the same person, whether natural or legal, and provided that these accounts are kept in the same company.	**Customer responsibility** Not applicable to AWS services.	Not applicable.
20.2 Payment transactions and transfers that present a low level of fraud risk, as a result of a risk analysis by transaction, are exempt from strong authentication, provided that the company complies with: **i.** Implement some of the payment industry standards, EMV 3DS and EMV payment tokenization, in their most recent versions.	**Customer responsibility** AWS customers are responsible for their payment fraud detection and exemption management processes. *Implementing Payment Industry Standards:* AWS does not directly provide or manage payment processing capabilities. However, AWS offers services such as AWS Marketplace that can help customers find and integrate third-party payment solutions that support the latest industry standards such as EMV 3DS and EMV tokenization.	Not applicable.

Summary of requirements	AWS Considerations	Implementation
ii. Define the threshold amount per transaction below which the exemption for the above-mentioned risk analysis will apply. **iii.** Periodically measure the fraud rate of payment transactions by channel and type of transaction. **iv.** Periodically update the applicable rules in risk analysis based on the fraud risk indicator. **v.** Use the data that is available for each type of operation, including, but not limited to, those associated with the user's behavior, the medium used and those that can be obtained from it for the purpose of risk analysis.	AWS customers are responsible for selecting, implementing, and maintaining the appropriate payment processing solutions that meet the industry standards. *Defining Exemption Thresholds:* The transaction value thresholds for authentication exemption is a customer-specific decision based on their risk appetite and fraud monitoring data. AWS can provide guidance and architectural recommendations to help customers integrate their payment processing solutions with their transaction monitoring and risk analysis capabilities. *Measuring Fraud Rates:* AWS customers are responsible for monitoring and measuring the fraud rates for their payment transactions across different channels and transaction types. AWS provides services such as Amazon Fraud Detector and Amazon GuardDuty that AWS customers can use to detect and investigate suspicious payment activities. However, the specific fraud measurement and reporting processes must be implemented by the AWS customer. *Updating Risk Analysis Rules:* AWS customers are responsible for periodically updating their risk analysis rules based on fraud indicators. AWS can provide guidance on best practices for building adaptable, rules-based fraud detection models using services such as Amazon Fraud Detector. However, the actual definition and tuning of the risk analysis rules is the AWS customer's responsibility. *Using Transaction Data:* AWS customers are responsible for collecting and analyzing the relevant transaction data such as user behavior or device information to feed into their risk analysis models. AWS can provide services such as Amazon Athena and Amazon Redshift to help customers store, process, and analyze large volumes of transaction data. However, the specific data sources and analysis workflows must be implemented by the AWS customer.	

Summary of requirements	AWS Considerations	Implementation
20.3 The company shall be liable for losses, unless it can substantiate the user's responsibility, for transactions not recognized by customers that have been executed through digital channels without adhering to the enhanced authentication requirement, or under the exemption specified in paragraph 20.2 of this article, or that were executed after the user reported the theft or loss of their credentials.	**Customer responsibility** Not applicable to AWS services.	Not applicable.

Article 21. Use of APIs for the provision of online services.

Summary of requirements	AWS Considerations	Implementation
21.1 The use of application programming interfaces, to provide services to perform operations, through third-party services, requires that the following measures be implemented: **a)** Analyze associated risks and implement mitigation measures. **b)** Mutual authentication of systems and users. **c)** The authorization of operations by users. **d)** The encryption of data in storage or during transmission. **e)** Secure API development practices and review of secure coding practices. **f)** Vulnerability analysis and penetration testing. **g)** The security of the technological infrastructure that supports it. **h)** Failure tolerance and contingency mechanisms.	**Customer responsibility** AWS customers have responsibility for their application programming interfaces (APIs) and their API-based integrations and security. AWS can provide guidance, tools, and services to support customers in meeting the API security requirements. *Risk Analysis and Mitigation:* AWS customers are responsible for conducting a comprehensive risk assessment of their API-based integrations and implementing appropriate mitigation measures. AWS provides services such as AWS Config, AWS Security Hub, and Amazon GuardDuty to help customers identify and mitigate risks in their cloud environments. *Mutual Authentication:* AWS Identity and Access Management (IAM) enables customers to implement mutual authentication between systems and users accessing APIs. Customers can use IAM roles, policies, and AWS-managed keys to achieve secure, authenticated access to their APIs. *Authorization of Operations:* IAM helps AWS customers define and enforce fine-grained access control policies to authorize specific API operations for users and systems. AWS customers can use IAM to implement the principle of least privilege for their API-based integrations. *Data Encryption:* AWS offers a wide range of encryption options, including encryption at rest and in transit, for data accessed through APIs. AWS customers can use services such as AWS Key Management Service (AWS KMS), AWS CloudHSM, and SSL/TLS to encrypt data and secure API communications. *Secure Coding and Vulnerability Management:*	*Risk analysis and mitigation:* SEC 1 - Secure Operations Includes processes for risk assessment and implementing security controls to mitigate identified risks. *Mutual authentication:* SEC 2 - Authentication Covers implementing secure authentication mechanisms for both systems and users. *Authorization of operations:* SEC 3 - Authorization and Access Control *Data encryption:* SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit *Secure API development:* SEC 1 - Secure Operations Includes secure coding practices and application security reviews. *Vulnerability analysis and testing:* SEC 1 - Secure Operations Covers vulnerability management and penetration testing. *Infrastructure security:* SEC 5 - Network Protection

Summary of requirements	AWS Considerations	Implementation
i) Access control in the data environment, systems and infrastructure. **j)** Monitoring of information security events and managing them when they constitute incidents.	AWS customers are responsible for implementing secure coding practices and performing vulnerability assessments for their API implementations. AWS provides guidance, tools, and services such as AWS WAF or Amazon Inspector to help customers build and test secure APIs. *Infrastructure Security, Failure Tolerance, and Access Control:* AWS manages the security of the underlying cloud infrastructure, but AWS customers are responsible for securing their own API-based applications and integrations. AWS customers can use AWS services such as Amazon Virtual Private Cloud (VPC), Amazon CloudWatch, and AWS Identity and Access Management (IAM) to implement security controls for their API environment. *Monitoring and Incident Management:* AWS customers can use AWS services such as Amazon CloudWatch, AWS CloudTrail, and Amazon GuardDuty to monitor their API-based integrations for security events and incidents. AWS provides guidance and best practices to help customers establish effective incident response and management processes.	SEC 6 - Compute Protection Secure the underlying infrastructure. *Failure tolerance and contingency:* REL 4 - Design Interactions to Prevent Failures REL 5 - Design Interactions to Mitigate Failures Enables fault tolerance and contingency planning. *Access control:* SEC 3 - Authorization and Access Control Define and implement access control policies. *Monitoring and incident management:* SEC 10 - Incident Response OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events Covers security event monitoring and incident response.

Summary of requirements	AWS Considerations	Implementation
21.2 The company must take international standards and reference frameworks as a reference, and when it is feasible to adopt them within the framework of trade union or sectoral agreements, for the implementation of data exchange and encryption, as well as the authentication and authorization of operations, without this being a restrictive list. **21.3** The technical specifications of the APIs used must be documented in such a way as to facilitate their auditing and the implementation necessary for their use.	**Customer responsibility** AWS customers are responsible for documenting and aligning their API-based integrations with relevant international and industry standards. *Aligning with International Standards:* AWS is certified under a wide range of international security and compliance standards, including: • ISO 27001, ISO 27017, ISO 27018 • PCI DSS • NIST Cybersecurity Framework • HIPAA AWS customers can use the certifications obtained by AWS to help meet their own regulatory and industry requirements for data exchange, encryption, authentication, and authorization. AWS also provides guidance on how to use its services to implement controls aligned with standards such as NIST 800-63 for digital identity. *Adopting Sector-Specific Standards:* AWS encourages customers to collaborate with their industry peers and trade associations to adopt common, sector-specific standards and frameworks for API integration. AWS can provide architectural guidance and technical assistance to help customers implement standards-based API solutions within their industry context. *Documenting API Technical Specifications:* AWS customers are responsible for thoroughly documenting the technical specifications of the APIs they use, including those provided by AWS services. AWS customers can also use AWS service-level agreements (SLAs) and other technical details to supplement their API documentation. AWS publishes comprehensive API reference documentation for all its services, which AWS customers can use as a starting point for their own API documentation. *Facilitating API Auditing:*	Not applicable.

Summary of requirements	AWS Considerations	Implementation
	The detailed API documentation provided by AWS customers can help facilitate auditing and monitoring of the API-based integrations. AWS provides services such as AWS CloudTrail, Amazon CloudWatch, and AWS Config to help AWS customers track and audit the usage and configuration of their API-based resources.	
21.4 Companies must implement the necessary measures to ensure that the third party authorized by the user accesses only the information indicated by the user.	**Customer responsibility** AWS customers can use the access control, authorization, and monitoring capabilities provided by AWS services such as AWS Identity and Access Management (IAM), Resource-Based Policies, and AWS CloudTrail to implement a user-centric third-party access management solution. The specific implementation and enforcement of access policies is the AWS customer's responsibility *Access Control:* AWS Identity and Access Management (IAM) helps define granular access control policies that grant specific permissions to third-party services and applications. AWS customers can use IAM to limit the scope of access for third-party integrations; to verify that third parties only have permission to access the necessary resources and data. *Fine-Grained Authorization:* AWS provides fine-grained authorization mechanisms, such as AWS Resource-Based Policies and IAM Policies, that AWS customers can use to explicitly define the actions and resources that third-party integrations are allowed to access. AWS customers can use these controls to verify third-party access is restricted to only the information and operations that the user has authorized. *Attribute-Based Access Control:* AWS supports attribute-based access control (ABAC), which allows AWS customers to create dynamic access control policies based on attributes associated with the user, resource, or environment. AWS customers can use ABAC to enforce access control rules that are tailored to the specific context of the third-party integration and the user's authorization. *Monitoring and Auditing:*	*Third-party access to information:* SEC 3 - Authorization and Access Control This practice covers implementing fine-grained access control policies to limit the scope of access for third-party applications and services. AWS customers can: Define authorization policies that specify the exact data and resources the third-party is allowed to access. Enforce these policies through appropriate access control mechanisms. Tie the authorized access to the user's own permissions and consent. SEC 2 - Authentication Authenticating that third-party applications and services accessing the data are legitimate entities. SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit Protecting the confidentiality and integrity of the data being accessed, both at rest and in transit. SEC 10 - Incident Response

Summary of requirements	AWS Considerations	Implementation
	AWS CloudTrail and Amazon CloudWatch are designed to provide comprehensive logging and monitoring capabilities to track all API calls and user activities, including those made by third-party integrations. AWS customers can use these services to monitor and audit third-party access to validate it aligns with the user's authorization.	Enabling the ability to quickly detect, investigate, and respond to any unauthorized access attempts by third-parties. *Additional considerations:* SEC 1 - Secure Operations Incorporating access control and data protection measures into the overall security operations. OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events Monitoring the interactions between users, third-parties, and the data or resources for anomalies.

SUBCHAPTER IV PROVISION OF THIRD-PARTY SERVICES

Article 22. Services provided by third parties.

Summary of requirements	AWS Considerations	Implementation
In the case of services provided by third parties in aspects related to information technology management, information security management or data processing, the company, in addition to complying with the requirements established in the Corporate Governance and Integral Risk Management Regulations and the Regulations for Operational Risk Management, must: **a)** Assess information security threats and vulnerabilities in the provision of goods and services and implement treatment measures. **b)** Ensure that the contractual arrangement with the supplier and its implementation allow it to comply with the obligations established in these Regulations.	**Shared responsibility** AWS customers can use the security capabilities, compliance programs, and contractual frameworks provided by AWS to address specific third-party service requirements outlined in the regulation. However, the ultimate responsibility for assessing risks, ensuring contractual compliance, and defining roles and responsibilities lies with the AWS customer. *Assessing Threats and Vulnerabilities:* AWS customers are responsible for assessing the security threats and vulnerabilities associated with third-party services. AWS provides a wide range of security services and tools such as Amazon GuardDuty, AWS Security Hub, or AWS Inspector that AWS customers can use to identify, assess, and mitigate risks in their cloud environment. AWS customers can also use AWS compliance reports and certifications to understand the security controls in place for AWS services. *Ensuring Contractual Compliance:* AWS offers an AWS Enterprise Agreement designed specifically for financial services customers to help them meet regulatory requirements. The AWS Enterprise Agreement includes terms and conditions that address the AWS customer's obligations under regulations, including the ability to comply with requirements in this regulation. AWS customers can work with their AWS account team to review the AWS Enterprise Agreement and determine whether it meets their specific needs. *Defining Roles and Responsibilities:*	*Assess and treat information security threats and vulnerabilities:* SEC 1 - Secure Operations Processes for identifying, assessing, and mitigating risks related to suppliers and third-party services. Implementing appropriate security controls to address the identified threats and vulnerabilities. *Contractual compliance:* SEC 1 - Secure Operations Review and validate that supplier contracts and implementation meet regulatory requirements. *Establish roles and responsibilities:* SEC 1 - Secure Operations Define the information security roles and responsibilities of the supplier in the contract. *Additional relevant practices:* SEC 2 - Authentication Securing the authentication and access controls for the supplier's personnel. SEC 3 - Authorization and Access Control

Summary of requirements	AWS Considerations	Implementation
c) Establish the roles and responsibilities that the provider contractually assumes regarding information security and ensure that the company carries out the corresponding complementary implementations to meet the requirements of this Regulation.	The AWS Enterprise Agreement clearly delineates the respective responsibilities of AWS and the AWS customer for security and compliance. AWS customers can use this information to establish the specific roles and responsibilities that AWS assumes, as well as the complementary responsibilities the AWS customer must fulfill. AWS also provides detailed documentation on the AWS Shared Responsibility Model to help AWS customers understand their security and compliance accountabilities.	Defining and enforcing the appropriate authorization policies for supplier access. SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit Data protection controls for data shared with or accessed by suppliers. SEC 10 - Incident Response Coordinating incident response processes with suppliers to identify and mitigate issues.

Article 23. Use of cloud services.

Summary of requirements	AWS Considerations	Implementation
To use cloud services, the company must implement information security policies and procedures that are of specific application, that take into account a framework of international good practices for the use of these services, and that, in addition to the requirements of Article 22 of the Regulation, include the following aspects: **a)** Information security requirements that cloud services must comply with and procedures to ensure implementation before use. **b)** Guidelines for network segregation that allow the isolation of company information from that of third parties in the shared environment of the cloud service. **c)** Evaluation of the availability of event logs offered by the cloud service provider and meeting the need for additional logs for information security monitoring. **d)** Provision of a training plan for management levels, administrators of these services, personnel in charge of their implementation and those who make use of them, on what is necessary to manage information security in these services.	**Customer responsibility** AWS customers are responsible for defining and implementing their information security policies and procedures for cloud services, and they can employ the security capabilities, compliance programs, and training resources provided by AWS. *Security Requirements and Implementation:* AWS customers are responsible for defining the specific information security requirements for their use of cloud services. AWS provides a wide range of security services, features, and compliance programs that customers can use to meet their security requirements: • AWS Security Hub for comprehensive security assessment. • AWS Config for configuration monitoring. • AWS Artifact for access to compliance reports and certifications. *Network Segregation and Isolation:* Amazon Virtual Private Cloud (VPC) allows customers to create isolated, private networks within the AWS Cloud. AWS customers can use VPC features such as security groups, network ACLs, and VPN connections to logically segregate and isolate their information from other AWS customers. AWS also provides advanced networking capabilities to enable secure connectivity between on-premises and cloud environments. *Event Logging and Monitoring:* AWS CloudTrail is designed to log of API calls and user activities within the AWS environment. AWS customers can use AWS CloudTrail, along with other services such as Amazon CloudWatch, to collect, monitor, and analyze events and logs. AWS also provides the flexibility for AWS customers to implement additional logging and monitoring capabilities as needed.	*Information security requirements:* SEC 1 - Secure Operations Define and validate the security requirements for cloud services used, including compliance with relevant standards and regulations. Implement necessary security controls and processes before deploying cloud services. *Network segregation and isolation:* SEC 5 - Network Protection Establish network segmentation and isolation to separate the company's information from third-parties in a shared cloud environment. *Event logging capabilities:* SEC 10 - Incident Response OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events Assessing the logging and monitoring capabilities provided by the cloud service, and implementing additional logging as needed to support security monitoring. *Training for cloud service management:* SEC 1 - Secure Operations

Summary of requirements	AWS Considerations	Implementation
	Training and Awareness: AWS offers a wide range of training resources, including online courses, whitepapers, and hands-on labs, to help customers and their teams develop the necessary skills to manage information security in the cloud. AWS customers can use the AWS training offerings as part of their overall training plan for cloud service administrators, implementers, and users.	Develop and deliver targeted training programs for cloud service administrators, implementers, and users to facilitate effective security management. *Additional considerations:* SEC 2 - Authentication SEC 3 - Authorization and Access Control SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit

Article 24. Significant data processing services.

Summary of requirements	AWS Considerations	Implementation
24.1 The contracting of a significant service provided by third parties for data processing, including cloud services, should be considered as an important change in the IT environment, with the definition of significant service established in the Corporate Governance and Integral Risk Management Regulations and the current regulations associated with new products and important changes being applicable. **24.2** The company must comply with the following aspects related to the contracting of a significant service provided by third parties for data processing, including cloud services, in addition to the provisions of articles 22 and 23 of these Regulations, as appropriate: **a)** Ensure adequate access to information, at reasonable times and upon request only, by the Superintendency, Internal Audit, and the External Audit Firm, under normal operating conditions and under special regimes. **b)** Manage information security incidents, in accordance with paragraph 6 of Article 12 and to carry out the planned activities provided for in Article 13 of these Regulations, as applicable to the significant data processing service in question.	**Customer responsibility** AWS customers are responsible for implementing appropriate controls, processes, and strategies for their specific regulatory and business requirements. *Access to information:* AWS customers maintain full control and ownership of their data and content hosted on AWS. AWS customers can grant authorized access to their data and resources, including to regulators, internal and external auditors as required. AWS customers can use AWS services such as AWS CloudTrail, AWS Config, and AWS Artifact to monitor, audit, and provide evidence of their AWS environment. *Incident management:* AWS has a formal, documented incident response policy and program to manage security incidents. AWS customers are responsible for monitoring their own environments and responding to incidents, and must have their own incident response procedures designed for the AWS environment. AWS customers can use AWS services such as Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub to monitor, audit, and provide evidence of their AWS environment. *Exit strategy:* AWS customers are responsible for having an exit strategy and plan to migrate data and workloads off AWS if needed. The AWS Enterprise Agreement includes terms to support a smooth exit process for customers. AWS provides features such as AWS Snowball and Database Migration Service to facilitate data migration.	*Access for oversight bodies:* SEC 3 - Authorization and Access Control Implement access control policies and mechanisms to grant the Superintendency, internal audit, and external audit firms access to relevant information and systems. SEC 1 - Secure Operations Establish processes to facilitate access requests and support compliance with regulatory requirements. *Manage information security incidents:* SEC 10 - Incident Response Define and implement incident management processes that align with the regulatory requirements for significant data processing services. OPS 8 - Health of a Workload OPS 9 - Health of Operations OPS 10 - Workload and Operations Events Monitoring the cloud services for security incidents and events. *Exit strategy:*

Summary of requirements	AWS Considerations	Implementation
c) Have an exit strategy for services under the responsibility of the provider that allows you to resume operations on your own account or through another provider. Such a strategy must include, among other aspects, the actions necessary for the migration of information to the resources of the company or another provider.		Develop a comprehensive exit strategy that includes plans for migrating data and resuming operations in the event of a provider change or service termination. SEC 8 - Data Protection at Rest SEC 9 - Data Protection in Transit Verify data protection controls are in place to facilitate the secure migration of information. *Additional considerations:* SEC 2 - Authentication SEC 3 - Authorization and Access Control Control access to the cloud environments and data during the exit process. REL 11 - Resiliency Implementation Verify the resilience of the exit strategy and migration processes.
24.2 (continued) The company must comply with the following aspects related to the contracting of a significant service provided by third parties for data processing, including cloud services, in addition to the provisions of articles 22 and 23 of these Regulations, as appropriate: **d)** Keep an inventory of the services that the supplier, in turn, contracts with third parties (chain contracting) and that are related to the services contracted by the company.	**Shared responsibility** AWS customers are responsible for implementing the appropriate controls, processes, and contract terms to meet their regulatory and business requirements. *Inventory of subcontracted services:* AWS customers are responsible for maintaining an inventory of the services that AWS as primary service provider has subcontracted to third parties. The inventory allows the customer to understand the full chain of providers involved in delivering the contracted services.	Not applicable.

Summary of requirements	AWS Considerations	Implementation
e) Ensure that confidential information in the supplier's custody is permanently deleted upon termination of the contractual agreement.	AWS offers an AWS Enterprise Agreement designed specifically for financial services customers to help them meet regulatory requirements. The AWS Enterprise Agreement includes terms and conditions that address the customer's obligations under regulations, including the ability to comply with requirements in this regulation. *Deletion of confidential data:* AWS offers an AWS Enterprise Agreement designed specifically for financial services customers to help them meet regulatory requirements. The AWS Enterprise Agreement includes terms and conditions that address the customer's obligations under regulations, including the ability to comply with requirements in this regulation. AWS customers maintain full ownership and control of their data stored in the AWS environment. Upon termination of the service agreement, customers are responsible for ensuring their data is securely deleted from the AWS environment. AWS provides customers the ability to encrypt their data and manage their own encryption keys. This enables AWS customers to maintain control over their data, including secure deletion upon exit.	
24.2 (continued) The company must comply with the following aspects related to the contracting of a significant service provided by third parties for data processing, including cloud services, in addition to the provisions of articles 22 and 23 of these Regulations, as appropriate:	**Customer responsibility** AWS customers are responsible for verifying that AWS controls meet their regulatory and security requirements. AWS customers must review the reports and certifications periodically to maintain compliance. *Verification of security controls:* AWS customers are responsible for verifying that AWS, as their cloud services provider, has appropriate security controls in place, in accordance with applicable regulations. AWS provides a wide range of audit reports and certifications that customers can review, including SOC, ISO, and PCI reports.	Not applicable.

Summary of requirements	AWS Considerations	Implementation
f) Verify annually that the data processing service provider has information security controls, in accordance with current information security regulations, as applicable to the service provided. This can be supported by independent reports and audit reports that include within their scope the verification of such controls. **g)** When it comes to cloud services, to comply with what is required in the previous paragraph, the company must annually demonstrate that the provider maintains current ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 certifications, and that it has a SOC 2 type 2 report or other equivalents, relevant to the service provided and to the area or region from which the service is provided.	AWS customers can use independent audit reports and certifications to assess the controls provided by AWS. *Cloud-specific security requirements:* AWS maintains all of these key security certifications, ISO 27001, ISO 27017, and ISO 27018 and provides SOC reports. AWS customers can access the relevant audit reports through AWS Artifact. AWS customers can review these reports to validate the security controls in place for AWS services they use.	
24.3 The company must inform this Superintendency about the contracted service, the provider involved, the agreed service levels, the technological infrastructure used, as well as the procedures and managers to comply with letters a) to f), and as appropriate g) of the previous paragraph; a maximum of thirty (30) calendar days after starting the provision of data processing.	**Customer responsibility** AWS customers are responsible for notifications or requests for authorization to regulators.	Not applicable.

Article 25. Authorization for contracting a significant data processing service provided by third parties.

Summary of requirements	AWS Considerations	Implementation
25.1 The company must request authorization from the Superintendency, prior to contracting a significant data processing service provided by third parties from abroad, if such service has limitations to meet the requirements established in paragraph 24.2 of article 24 of these Regulations, which will be answered by the Superintendency within sixty (60) business days. To request such authorization, companies must submit, together with their request, a report with the legal basis for the limitations identified and a proposed plan for the implementation of compensatory measures. **25.2** The authorization granted by this Superintendency is specific to the service provider and, to the country and city from which it is received, as well as to the general conditions that were the subject of the authorization, so if there are modifications to them and, if the limitation mentioned in the previous paragraph is maintained, a new authorization procedure is required before the Superintendency.	**Customer responsibility** AWS customers are responsible for notifications or requests for authorization to regulators.	Not applicable.

SUBCHAPTER V SIMPLIFIED FRAMEWORK OF THE ISMS-C

Article 26. Simplified Information Security Management System.

Summary of requirements	AWS Considerations	Implementation
26.1 The simplified information security management regime requires the planning and execution of the following minimum activities, whose frequency must be at least annual: **a)** Identify with the business and support units the most important information, due to existing regulatory or contractual obligations, and because of the need to operate. **b)** Identify the devices that connect to the internal network and any software that is installed in the technological infrastructure, and ensure that they are in accordance with a previously established secure configuration.	**Customer responsibility** These activities are the AWS customer's responsibility as part of their overall information security management program. AWS customers must perform these activities at least annually to maintain an updated view of their critical information assets and technology environment. AWS customers retain responsibility for managing and securing their own applications, data, and connected devices, using the security capabilities provided in the AWS Cloud. Identify critical information assets: AWS customers are responsible for identifying their critical information assets, based on regulatory and contractual obligations and operational needs. Information assets can include: customer data, financial records, intellectual property. The AWS customer must document and maintain an inventory of these critical information assets. Identify and secure connected devices/software: AWS customers must identify all devices such as laptops, servers, IoT devices, that connect to their internal network and must also identify all software installed in their technology infrastructure. AWS customers must verify these devices and software are configured securely, based on established security baselines and policies for patch management, applying security configurations, and restricting unnecessary access or capabilities, among others.	Not applicable.

Summary of requirements	AWS Considerations	Implementation
26.1 (continued) The simplified information security management regime requires the planning and execution of the following minimum activities, whose frequency must be at least annual: **c)** Identify user accounts with access permissions enabled and in particular those with administrative privileges with the possibility of adding software to the infrastructure, and maintaining the principle of minimum privileges granted. **d)** Implement and maintain a security baseline in operating systems and applications used, including those corresponding to mobile devices, workstations, servers and communication devices. Identify and evaluate the enablement of security features integrated into operating systems. **e)** Prioritize and manage identified security vulnerabilities, for whose timely identification you must have the necessary information services. **f)** Develop a guidance campaign for the adoption of safe practices aimed at employees, management and management.	**Customer responsibility** AWS customers can use the security capabilities and services provided by AWS for their information security management program, but AWS customers retain responsibility for the implementation and execution of these activities. *Manage user accounts and privileges:* AWS customers must identify all user accounts with access permissions, especially those with administrative privileges. AWS customers must maintain the principle of least privilege, only granting the minimum access required for each user. This helps limit the potential impact of a compromised user account. *Implement security baselines:* AWS customers must establish and maintain security baselines for their operating systems and applications. This includes mobile devices, workstations, servers, and communications equipment. AWS customers must identify and enable the security features built into the operating systems. *Manage security vulnerabilities:* AWS customers must have processes to prioritize and remediate identified security vulnerabilities. This requires access to timely vulnerability information and intelligence services. Proper vulnerability management helps reduce the attack surface and risk exposure. *Security awareness and training:* Educating users on secure practices is crucial to an effective security program. AWS customers can develop and deliver security guidance and awareness campaigns that target employees, management, and leadership.	*Manage user accounts and privileges:* SEC 3 - Authorization and Access Control Implementing the principle of least privilege by carefully managing user accounts and access permissions, especially for administrative privileges. Regularly reviewing and auditing user access to verify it aligns with the business requirements. *Implement security baselines:* SEC 1 - Secure Operations Establishing and maintaining security baselines for operating systems, applications, mobile devices, servers, and network devices. Using the security features and controls. *Manage security vulnerabilities:* SEC 1 - Secure Operations Implementing vulnerability management processes to identify, assess, prioritize, and remediate security vulnerabilities in a timely manner. Utilizing relevant information services to stay informed of the latest vulnerabilities. *Security awareness and training:* SEC 1 - Secure Operations Creating and delivering targeted security awareness and training programs for employees, management, and other relevant stakeholders. Promoting the adoption of secure practices within the organization.

Summary of requirements	AWS Considerations	Implementation
		Additional considerations: SEC 2 - Authentication Securing the authentication mechanisms used to access systems and applications. SEC 5 - Network Protection SEC 6 - Compute Protection Securing the underlying compute infrastructure. SEC 10 - Incident Response Integrating security controls and processes into the overall incident management capabilities.
26.2 If the company provides any of the operations indicated in Article 19 of these Regulations through digital channels, as far as their implementation is concerned, it must comply with the provisions established in Subchapter III of Chapter II of these Regulations.	**Customer responsibility** See the AWS considerations for Subchapter III of Chapter II in this document.	Not applicable.
26.3 If it uses significant services provided by third parties, as appropriate to their implementation, the company must comply with the provisions established in Subchapter IV of Chapter II of these Regulations.	**Customer responsibility** See the AWS considerations for Subchapter IV of Chapter II in this document.	Not applicable.

Summary of requirements	AWS Considerations	Implementation
26.4 The company must maintain a cybersecurity program, in accordance with Subchapter II of Chapter II of these Regulations, with a scope that at least includes the services indicated in paragraphs 26.2 and 26.3 of Article 26 of these Regulations.	**Customer responsibility** See the AWS considerations for Subchapter II of Chapter II in this document.	Not applicable.

SUBCHAPTER VI ENHANCED FRAMEWORK OF THE ISMS-C

Article 27. Additional requirements for a company with market concentration.

Summary of requirements	AWS Considerations	Implementation
27.1 The board must appoint a director responsible for ensuring the effectiveness of the information security management system, including the development of the SGSI-C strategic plan. **27.2** The company must periodically submit to an independent evaluation of the scope and effectiveness of the SGSI-C; such evaluation may be carried out by the internal audit unit or other team that meets the requirement of independence, provided that it has previous experience and international certifications that demonstrate the necessary technical preparation.	**Customer responsibility** Appointments to the board and internal evaluations of the SGSI-C are responsibilities of the AWS customers. AWS provides the security capabilities and services to support the AWS customer's information security program, but the overall governance, oversight, and independent assessment is the customer's obligation. AWS customers can use AWS audit reports and certifications as part of their independent evaluation process.	Not applicable.

Document revisions

Date	Description
May 2024	Initial draft.
September 2024	First publication.