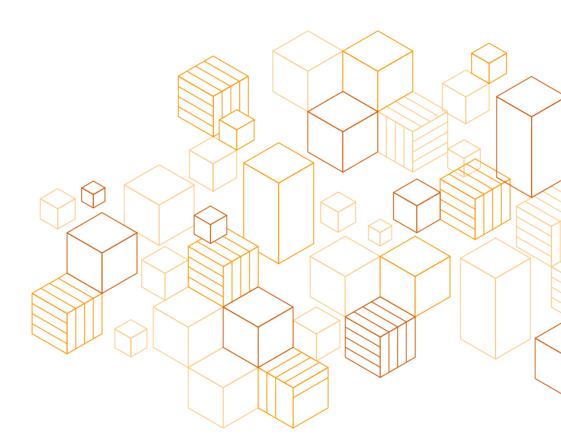
# AWS User Guide to Financial Services Regulations in Argentina

Central Bank of Argentina (BCRA) Communications "A" 6,354 and 6,375

May 2020





#### **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.

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Contents

Overview	1
Security and Shared Responsibility	2
Security in the Cloud	3
Security of the Cloud	4
AWS Compliance Programs	5
Certifications and Third-Party Attestations	5
AWS Artifact	7
AWS Global Infrastructure	7
BCRA Regulation	8
Outsourcing by Financial Institutions	8
Technical and Operational Requirements	10
Getting Started	12
Additional Resources	12
Document Revisions	13
Appendix: AWS Considerations for the Technical and Operational Require the BCRA Regulation	
Information Security Governance - Section 7.7.1	15
Awareness and Training – Section 7.7.2	22
Access Control - Section 7.7.3	25
Integrity and Registration - Section 7.7.4	30
Monitoring and Control - Section 7.7.5	40
Incident Management - Section 7.7.6	44
Operational Continuity - Section 7.7.7	48

#### About this Guide

This document provides information to assist banks and financial services institutions in Argentina regulated by the Central Bank of Argentina (BCRA) as they adopt and accelerate their use of the Amazon Web Services (AWS) Cloud.

#### This guide:

- describes the respective roles that the customer and AWS each play in managing and securing the cloud environment;
- provides an overview of the regulatory requirements and guidance from BCRA that financial institutions can consider when using AWS;
- provides additional resources that financial institutions can use to design and architect their AWS environment to be secure and meet regulatory expectations, including under BCRA's regulations.

#### Overview

AWS provides financial services institutions across banking, payments, capital markets, and insurance the secure, resilient global cloud infrastructure and services they need to differentiate themselves today and adapt to the needs of tomorrow. Through continuous innovation, AWS delivers stringent security requirements, the greatest breadth and depth of services, deep industry expertise, and an expansive partner network. Building on AWS empowers organizations to modernize their infrastructure, meet rapidly changing customer behaviors and expectations, and drive business growth. AWS offers IT services in categories ranging from compute, storage, database, and networking to artificial intelligence and machine learning. Across the world, financial institutions have used AWS services to build their own applications for mobile banking, regulatory reporting and market analysis.

Banco Central de la República Argentina (BCRA) is the primary financial supervisory authority in Argentina responsible for the regulation, inspection, and supervision of financial institutions, including banking and credit institutions and payments processors (collectively, Fls or regulated entities).

In November 2017, BCRA issued <u>Communication "A" 6,354</u> (amended by <u>Communication "A" 6,375</u>) to update the general "outsourcing" guidelines that FIs regulated by BCRA must follow when outsourcing information technology (IT) services to a third-party technology provider, including the use of cloud services (the "BCRA Regulation"). In addition, BCRA has published regulatory guidance through several public <u>Normative Interpretations</u> (or Interpretaciones Normativas) available on its <u>website</u>. These <u>Normative Interpretations</u> have clarified the scope of the BCRA Regulation with respect to FIs' outsourcing to cloud service providers (CSPs).

The BCRA Regulation defines, among other things, the minimum technical and operational requirements that FIs should put in place for the management, implementation, and control of risks related to information technology, information systems, and other resources when outsourcing IT services to a third-party service provider, including the use of cloud services.

This guide is intended to be a resource to help FIs understand those technical and operational requirements under the BCRA Regulation when they use AWS. This guide includes a description of the AWS compliance framework and advanced tools and security measures, which FIs can use to evaluate, meet, and demonstrate compliance with their applicable regulatory requirements under the BCRA Regulation.

A full analysis of the BCRA Regulation is beyond the scope of this guide. However, the sections outlined below address the considerations that most frequently arise in interactions



1

with FIs in Argentina and provide information that FIs can use to better understand their and AWS' responsibilities with regards to the BCRA Regulation:

- Security and Shared Responsibility: It is important that FIs understand the AWS
   Shared Responsibility Model before exploring the specific technical and operational
   requirements outlined in the BCRA Regulation. The AWS Shared Responsibility Model
   is fundamental to understanding the respective roles of the customer and AWS for
   security, and informs the steps FIs need to take to ensure they comply with the BCRA
   Regulation.
- 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. BCRA has
  acknowledged in several Normative Interpretations that the regulated entities may rely
  on third-party audit reports, certifications, and other mechanisms to monitor and audit
  the services outsourced to a CSP. Customers can leverage 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. The AWS Global Cloud Infrastructure offers AWS customers an easier and more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to design an AWS environment consistent with their business and regulatory needs, including any applicable requirements under the BCRA Regulation.
- BCRA Regulation: This section sets out common considerations for FIs that use AWS
  as they consider some of the key technical and operational requirements under the
  BCRA Regulation, and it describes how FIs can leverage AWS services and tools to
  comply with their applicable regulatory requirements. <u>Appendix: AWS Considerations</u>
  <u>for BCRA Regulation Requirements</u> provides a list of requirements and corresponding
  considerations.

# Security and Shared Responsibility

It is important that FIs understand the AWS <u>Shared Responsibility Model</u> before exploring the specific requirements under the BCRA Regulation. Cloud security is a shared responsibility. AWS manages security *of the cloud* by ensuring that AWS Cloud Infrastructure complies with global and regional regulatory requirements and best practices, but security *in the cloud* is the responsibility of the customer. What this means is that customers retain control of the security



program they choose to implement to protect their own content, applications, systems, and networks, as they would for applications in an on-premises data center.

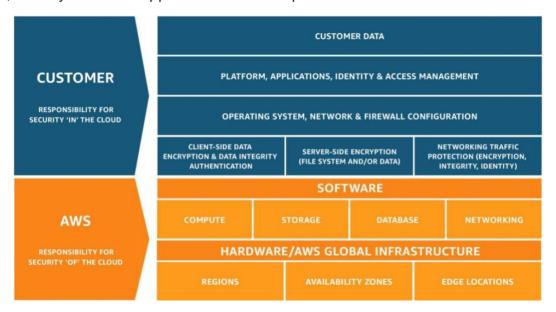


Figure 1: Shared Responsibility Model

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

#### **Security in the Cloud**

Customers are responsible for their security in the cloud. AWS customers are responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as any applicable network security controls. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that are used with the content.
- The country where their content is stored.



- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted, and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (laaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including 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 platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

#### **Security of the Cloud**

AWS's infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS's compliance certifications to validate the implementation and effectiveness of AWS's security controls, including internationally-recognized security best practices and certifications. You can learn more by downloading our whitepaper AWS & Cybersecurity in the Financial Services Sector.



The AWS compliance program is based on the following actions:

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

# **AWS Compliance Programs**

#### **Certifications and Third-Party Attestations**

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

**ISO 27001** is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System, which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the <u>ISO 27001</u> 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 information security controls implementation guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

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

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

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

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



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

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

For more information about other AWS certifications and attestations, see the <u>AWS</u> <u>Compliance Program</u> webpage. For information about general AWS security controls and service-specific security, see the <u>Amazon Web Services: Overview of Security Processes</u> whitepaper.

#### **AWS Artifact**

Customers can use <u>AWS Artifact</u> to review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

#### **AWS Global Infrastructure**

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



AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. More information on our disaster recovery recommendations is available at <a href="AWS">AWS</a> Disaster Recovery.

# **BCRA** Regulation

#### **Outsourcing by Financial Institutions**

The BCRA Regulation allows FIs to outsource—entirely or partially—to a third-party service provider a broad set of information technology services, including the use of cloud services.

Section 2 (Descentralización y tercerización de actividades) of the BCRA Regulation defines general considerations that FIs should consider when outsourcing IT services to a third-party service provider, including:

- 60 days' prior notification requirement (see <u>Notification</u> section).
- Conditions: including, among others, the technical and operational requirements that
  Fls may need to implement depending on the nature and type of the outsourced
  activities.
- Notification requirements: including a list of information that FIs need to submit to the regulator.
- FIs Responsibilities: FIs that decide to outsource services remain nevertheless responsible to comply with applicable laws and regulations, and rules issued by BCRA.

#### **Notification**

The BCRA Regulation (see Section 2 – Descentralización y tercerización de actividades) does not require FIs to obtain a formal approval from BCRA or the Superintendencia de Entidades Financieras y Cambiarias del Banco Central (SEFyC) prior to outsourcing IT services, but



instead FIs are required to notify such outsourcing to the SEFyC at least 60 calendar days prior to the commencement of the outsourced activities.<sup>1</sup>

#### **Regulator's Supervision and Oversight Powers**

BCRA has published regulatory guidance in the form of Normative Interpretations. This guidance has clarified the scope of the BCRA Regulation with respect to FIs' outsourcing to CSPs. In June 2019, BCRA published a Normative Interpretation that acknowledges that the review of international, third-party certifications (such as the ISO certifications) and independent third-party audit reports (such as the SOC reports) are generally sufficient to satisfy BCRA and SEFyC audit and access rights with respect to CSPs providing services to regulated entities. This clarification highlights how these third-party certifications, attestations, and audit reports are valuable compliance resources that benefit the FIs and the regulator in their oversight of the outsourced activities. For more information about these third-party certifications and audit reports, see the <a href="https://www.aww.numerica.com/www.aww.numerica.com/www.aww.numerica.com/www.aww.numerica.com/www.aww.numerica.com/www

AWS FI customers have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs, including any regulatory requirements.

Through an AWS Enterprise Agreement, AWS offers its FIs customers regulated by BCRA a contractual framework that helps them satisfy applicable contractual requirements under the BCRA Regulation, including specific terms that address a regulator's access and inspection rights, where required by applicable law and under certain conditions. For more information about AWS Enterprise Agreements, contact your AWS representative.

#### **Support Plans**

<u>AWS Support plans</u> are designed to give customer the right mix of tools and access to expertise so that customer can be successful with AWS while optimizing performance, managing risk, and keeping costs under control.

AWS Basic Support is included for all AWS customers and includes:

 Customer Service & Communities - 24x7 access to customer service, documentation, whitepapers, and support forums.

<sup>&</sup>lt;sup>1</sup> BCRA further clarified this notification requirement in its <u>Normative Interpretations</u>.



-

- <u>AWS Trusted Advisor</u> Access to the seven core Trusted Advisor checks and guidance to provision your resources following best practices to increase performance and improve security.
- <u>AWS Personal Health Dashboard</u> A personalized view of the health of AWS services, and alerts when your resources are impacted.

#### **Technical and Operational Requirements**

Section 7 (Servicios de tecnología informática tercerizados) of the BCRA Regulation describes the broad categories of IT activities that FIs may outsource to third-party service providers. Section 7 further outlines the general requirements and specific "technical and operational" controls that FIs may need to implement depending on, among other things, the nature and type of the outsourced activities.

#### Unified Point of Access (PAU, or Punto de Acceso Unificado)

Section 7.3.2.2 of the BCRA Regulation defines the Unified Access Point (Punto de Acceso Unificado, or PAU) and requires FIs to implement a non-operational environment that allows them to actively, continuously, and permanently control and monitor all the IT activities outsourced as well as their data. The PAU must be located in Argentina and managed by the FI. FIs can address the PAU requirement by leveraging the AWS Management Console and/or the AWS Command Line Interface (AWS CLI). The AWS Management Console provides a simple web interface for AWS services. It comprises and provides access to a broad collection of service consoles for managing AWS services, and provides an inbuilt user interface to perform AWS tasks. BCRA has clarified further the scope of this PAU requirement in its Normative Interpretations.

#### **Scenarios Matrix**

Section 7.5 of the BCRA Regulation outlines a "scenarios matrix," which describes four distinct IT outsourcing scenarios depending on the nature and types of data being handled, and the category of the outsourced services involved. BCRA assigns certain minimum technical and operational requirements to each of those scenarios.

Fls should consider the workload(s) under consideration, the relevant categories of data and services to be outsourced, and assess the materiality or criticality of the relevant workload(s) in light of the scenarios outlined in the BCRA Regulation and their operational risk management policies. As customers' requirements differ, AWS encourages each customer to obtain appropriate advice on their compliance with all regulatory and legal requirements that are



relevant to their business, including the minimum technical and operational requirements included in the BCRA Regulation, and other local regulations and laws.

The table below summarizes the scenarios matrix outlined in the BCRA Regulation:

		Minimum Technical and Operational Requirements						
Scenario	Situation	Info Sec	Awareness Training	Access Control	Integrity Registration	Monitoring Control	Incident Mgmt.	Continuity
ESD001	Customer data: use / exploitation, conservation, and transport, including financial transactions that hold customer data.	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD002	Accounting- financial data: use / exploitation, conservation, and transport, including or not customer data.	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD003	Financial transactions data: use / exploitation, conservation, and transport that does not include customer data.	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD004	Operational data: use / exploitation, conservation, and transportation that does not include accounting or financial information, customer data or financial transactions.	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023 RIR025	RMC003 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004

For further information on the technical and operational requirements described in the BCRA Regulation, see <a href="Appendix: AWS Considerations for the Technical and Operational Requirements under the BCRA Regulation">ARGULATION TO THE TECHNICAL AND TO THE TECHNICAL AND TO THE TECHNICAL AND THE TE



# **Getting Started**

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

For Fls in Argentina, next steps typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation
  of Compliance and Responsibility Summary, and ISO 27001 certification from the
  AWS Artifact portal (accessible via the AWS Management Console).
- Consider the relevance and application of the <u>AWS Security whitepapers</u>, and the CIS AWS Foundations Benchmark, as appropriate for your cloud journey and use cases. These industry-accepted best practices published by the Center for Internet Security go beyond the high-level security guidance already available, providing AWS users with clear, step-by-step implementation and assessment recommendations.
- Dive deeper on other governance and risk management practices as necessary in light of your due diligence and risk assessment, using the tools and resources referenced throughout this guide and in the Additional Resources section.
- Speak with your AWS representative to obtain additional information regarding the AWS Enterprise Agreement.

In addition to helping our customers maximize the use of the technology provided by AWS, the AWS technical team can support our customers so they can implement architecture, products, and services that allow them to meet any applicable technical and operational requirements under the BCRA Regulation.

#### Additional Resources

Set out below are additional resources to help Fls think about security, compliance and designing a secure and resilient AWS environment.



- AWS Compliance Quick Reference Guide: AWS has many compliance-enabling features that you can use for your regulated workloads in the AWS cloud. These features allow you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.
- AWS Well-Architected Framework: The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale application needs over time. The Well-Architected framework consists of five pillars: Operational Excellence; Security; Reliability; Performance Efficiency; Cost Optimization.

AWS has produced whitepapers addressing each pillar of the Well-Architected Framework, that are available here: <u>AWS Operational Excellent Pillar Whitepaper</u>; <u>AWS Security Pillar Whitepaper</u>; <u>AWS Reliability Pillar Whitepaper</u>; <u>AWS Performance Efficiency Whitepaper</u>; <u>AWS Cost Optimization Whitepaper</u>.

- Global Financial Services Regulatory Principles: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS cloud services and specifically, applying the shares responsibility model to their regulatory requirements. Customers can access a whitepaper on these principles under a non-disclosure agreement at <u>AWS Artifact</u>.
- 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 (i.e., security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS cloud offering's conformance to NIST CSF risk management practices (i.e., security of the cloud). Fls can leverage NIST CSF and AWS resources to elevate their risk management frameworks

For additional help, visit the Security, Identity and Compliance Whitepapers.

#### **Document Revisions**

Date	Description
May 2020	First publication



# Appendix: AWS Considerations for the Technical and Operational Requirements under the BCRA Regulation

The following sections list the technical and operational requirements identified under Sections 7.7.1 through 7.7.7 of the BCRA Regulation along with AWS considerations to assist FI customers understand each requirement when using AWS, and a description of the best practices from the <u>Well-Architected Framework</u> which FIs can use to support their compliance efforts.

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

The tables in the next sections are organized into the following columns:

- **Requirement:** This column lists the minimum technical and operational requirements (per category) that may be applicable to each of the scenarios outlined in the BCRA Regulation.
- AWS Considerations: This column explains the AWS considerations for addressing the requirements defined by BCRA. It
  may refer to the security and compliance of the cloud, and how AWS implements and manages the controls and/or AWS
  services FIs can use to address these requirements.
- Implementation Considerations: This column lists best practices for security in the cloud from the AWS Well-Architected Framework that FIs can implement as a starting point to support their compliance efforts. Details on each best practice and associated AWS services that customers may leverage can be found in the AWS Well-Architected Framework.

The following tables provide additional considerations on how customers can support their compliance efforts of their applicable requirements under the BCRA Regulation. These tables contain only a non-exhaustive sample of considerations. This is not legal or compliance advice. Customers should consult with their own legal and compliance teams.



### **Information Security Governance - Section 7.7.1**

These technical and operational requirements are related to the organization of strategic and operational management processes for information security, the functional and operational structure, and the determination of associated responsibilities.

Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGS001: Fls/service providers must establish and notify BCRA with a complete, exhaustive and updated,	Customer Responsibility Customers should define their operational model based on the AWS services and products they use.	Not applicable.
detailed description of the shared and/or exclusive responsibilities regarding the	As explained in the <u>Security and Shared Responsibility</u> section, cloud security is a shared responsibility. AWS manages security of the cloud ensuring AWS infrastructure complies with global regulatory requirements as well as best practices.	
responsibilities regarding the roles and functions for the administration and operational management of security of the information associated with the outsourced IT services (or "STI," as defined in the BCRA Regulation).	However, security in the cloud is the responsibility of the customer. This means that customers are responsible for the security programs they want to deploy to protect their content, applications, systems, and networks in the same way as they do in a local data center.	



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGS002: Fls/service provider must establish roles and functions for the processing of customer data, including the relevant responsibilities according to the level of participation and task being performed. These responsibilities must be formalized in the STI outsourcing agreements.	Shared Responsibility  AWS considers the FIs' definition of roles and responsibilities relating to how they will process their customers' data as an action for FIs to complete.  When using AWS services, customers maintain control over the entire life-cycle of their content on AWS, and are responsible for managing their content in accordance with their own specific needs, including content classification, access control, retention, and deletion.  AWS treats all Customer content and associated assets as critical information. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. We are vigilant about our customers' security and have implemented sophisticated technical and physical measures designed to prevent unauthorized access. AWS does not have meaningful visibility as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure.  In its agreements with customers, AWS makes specific security and privacy commitments that apply broadly to customer content in each Region the customer chooses to store its data. See Sections 3 and 4 of the AWS Customer Agreement.  AWS customers also have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs, including any regulatory requirements. For more information about AWS	
	Enterprise Agreements, contact your AWS representative.	



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGS003: Fls/service provider of the outsourced STI must comply with the laws and regulations related to the protection of personal data (Law 25.326) when the service involves the collection and use of personal data, which shall	Shared Responsibility As explained in the Security and Shared Responsibility section, it is important to note that when using AWS services, customers maintain control over their data and are responsible for managing critical content security requirements. This allows customers to control the entire life-cycle of their content on AWS and manage their content in accordance with their own specific needs, including content classification, access control, retention, and deletion.	Not applicable.
of personal data, which shall be reflected in the STI agreements.	For more information about the Shared Responsibility Model and its implications for the storage and processing of personal data using AWS, see the AWS whitepaper Using AWS in the Context of Common Privacy and Data Protection Considerations, and our Argentina Data Privacy website, which includes an overview of the Argentina Personal Data Protection Law No. 25,326 (PDPL) and common FAQs.	
	In its agreements with customers, AWS makes specific security and privacy commitments that apply broadly to customer content in each Region the customer chooses to store its data. The commitments AWS makes are consistent with the goals of the PDPL and Disposition 60-E/2016 to protect personal data.	
	AWS also offers an international Data Processing Addendum (DPA), also referred to as a data transfer agreement, which includes specific contractual commitments to adequately address the roles and obligations of each party with respect to the privacy and security of personal data.	
	For additional information on AWS Enterprise Agreements or the DPA, please contact your AWS representative.	



RGS004: FIs/service provider shall establish and document the exchange protocols of information among the participants of the STI agreement, including third parties subcontractors, as well as the techniques and operational measures (formats, time limits, responsible parties, etc.) that guarantee useful, timely, and complete  Customer Responsibility  Customers are responsible for defining the internal processes used to manage outsourced STIs.  To support FI customers, AWS develops and maintains customer support procedures that include metrics to verify performance. When a customer contacts AWS to report that AWS services do not meet their quality objectives, their issues are immediately investigated and, where required, commercially reasonable actions are taken to resolve them.  The customer support procedures that include metrics to verify performance. When a customer contacts AWS to report that AWS services do not meet their quality objectives, their issues are immediately investigated and, where required, commercially reasonable actions are taken to resolve them.  The customer support quality system includes, but is not limited to, procedures for reviewing and evaluating customer complaints, engaging necessary internal AWS resources and teams, and communicating the final disposition of the issue back to the	Requirement	Considerations	Implementation Considerations (Well Architected Practices)
information to the parties involved and to the BCRA.  AWS Support plans are designed to give customer the right mix of tools and access to expertise so that customer can be successful with AWS while optimizing performance, managing risk, and keeping costs under control.  AWS maintains procedures for notifying customers of customer-impacting issues using the AWS Service Health Dashboard. The AWS Service Health Dashboard publishes up-to-the-minute information on service availability, where customers can subscribe to an RSS feed to be notified of interruptions to each individual service and a full health history of each service.  In addition, the AWS Personal Health Dashboard gives customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and provides proactive notification to help customers plan for scheduled activities.	RGS004: Fls/service provider shall establish and document the exchange protocols of information among the participants of the STI agreement, including third parties subcontractors, as well as the techniques and operational measures (formats, time limits, responsible parties, etc.) that guarantee useful, timely, and complete information to the parties	Customer Responsibility Customers are responsible for defining the internal processes used to manage outsourced STIs.  To support FI customers, AWS develops and maintains customer support procedures that include metrics to verify performance. When a customer contacts AWS to report that AWS services do not meet their quality objectives, their issues are immediately investigated and, where required, commercially reasonable actions are taken to resolve them.  The customer support quality system includes, but is not limited to, procedures for reviewing and evaluating customer complaints, engaging necessary internal AWS resources and teams, and communicating the final disposition of the issue back to the customer.  AWS Support plans are designed to give customer the right mix of tools and access to expertise so that customer can be successful with AWS while optimizing performance, managing risk, and keeping costs under control.  AWS maintains procedures for notifying customers of customer-impacting issues using the AWS Service Health Dashboard. The AWS Service Health Dashboard publishes up-to-the-minute information on service availability, where customers can subscribe to an RSS feed to be notified of interruptions to each individual service and a full health history of each service.  In addition, the AWS Personal Health Dashboard gives customers a personalized view into the performance and availability of the services. It displays relevant and timely information to help customers manage events in progress, and provides proactive	,



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGS005: In the case of a service provider or subcontractor participating in	Customer Responsibility  AWS customers designate in which geographic region their content will be located.  With AWS, Fls can:	Not applicable.
an STI that processes, stores or transports data of the FI at locations abroad, the FI,	<ul> <li>Determine where their content will be stored, including the type of storage and geographic region of that storage.</li> </ul>	
service providers, and the third parties involved must provide the mechanisms necessary to verify whether the locations satisfy the legal provisions,	<ul> <li>Replicate and back up their content in more than one region, and AWS will not move or replicate customer outside of the Fl's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users. For current information on AWS Regions and Availability Zones, see Global Infrastructure.</li> </ul>	
regulations and contractual commitments established in the STI agreement, including	<ul> <li>Choose the secured state of their content. We offer FIs strong encryption for content in transit or at rest, and we provide FIs with the option to manage their own encryption keys.</li> </ul>	
the rules on "Expansion of financial entities."	<ul> <li>Manage access to their content and AWS services and resources through users, groups, permissions and credentials that FIs control.</li> </ul>	



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGS006: The STI agreement must include the obligation of non-disclosure of personal data and extend this obligation to subcontracted third parties.	Shared Responsibility  AWS gives customers ownership and control over their content through tools that allow customers to determine where their content will be stored, how it will be secured in transit or at rest, and how access to their AWS environment will be managed. AWS has implemented global privacy and data protection best practices in order to help customers establish, operate, and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.  The AWS ISO 27018 audit verifies the implementation of security controls that focus	SEC-7 Classify data SEC-8 Protect data at rest
	on protection of personal data. To learn more about AWS's ISO 27108 compliance, visit: ISO/IEC 27018:2019 Compliance. To learn more about data privacy on AWS, visit Data Privacy FAQ.  In its agreements with customers, AWS makes specific security and privacy commitments that apply broadly to customer content in each Region the customer chooses to store its data. For example, see Section 3 of the AWS Customer Agreement.  AWS customers also have the option to enroll in an Enterprise Agreement with AWS. Enterprise Agreements give customers the option to tailor agreements that best suit their needs. For more information about AWS Enterprise Agreements, contact your AWS representative.	



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGS007: Fls/service providers	Shared Responsibility	SEC-7 Classify data
must document and assign ownership of all information	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.	SEC-8 Protect data at rest
assets in the STI, determining the level of administrative responsibility and operational side of each party in the information life cycle.	AWS does not have meaningful visibility as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.	
	AWS provides an advanced set of access, encryption, and logging features to help FIs do this effectively (such as <a href="AWS CloudTrail">AWS CloudTrail</a> ). We do not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users.	
	In order to ensure asset management inventory and maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools.	
	AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. AWS is vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access.	
	AWS tracks, documents, and verifies media sanitization and disposal actions. All media removal and disposal is performed by designated AWS personnel.	
	Data Destruction: Content on drives is treated at the highest level of classification (Critical) per AWS Data Classification policy. Content is destroyed on storage devices as part of the decommissioning process in accordance with AWS security standards.	
	AWS hosts are securely wiped or overwritten prior to provisioning for reuse. AWS media is securely wiped or degaussed and physically destroyed prior to leaving AWS Secure Zones.	
	To validate AWS secure wipe processes and procedures, third-party auditors review the guidance within the AWS Media Protection policy, observe degaussing equipment and secure shred bins located within AWS facilities, observe historical tickets which tracked the destruction of a hard drive within a data center and the process of a device being wiped and removed from the environment.	



## **Awareness and Training – Section 7.7.2**

These technical and operational requirements are aimed at providing training and dissemination of IT security practices to develop preventive, detective, and corrective practices relating to security incidents that may arise in outsourced IT services.

Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RCC001: The content of the Awareness & Training (A&T) program should be formulated and kept updated based on an analysis of vulnerabilities and the results of Incident Management, and include, but not be limited to incidents: reported,	Shared Responsibility Customers are responsible for defining their own internal Training and Awareness program. However, Customers can leverage AWS training services and resources to ensure their staff have the appropriate training and resources to manage the AWS services. Training offerings can be found at Training and Certification.	OPS-1 Determine priorities  SEC-4 Detect and investigate security events  SEC-10 Respond to an incident
detected, and known.  RCC002: The content of the A&T program must include: detection and prevention of appropriation of personal data and credentials through attacks such as "Social engineering," "phishing," "vishing," and others with similar characteristics.	AWS has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.  The security awareness and training policy and procedures are reviewed and updated at least annually, or sooner if required due to information system changes.	OPS-1 Determine priorities  SEC-4 Detect and investigate security events  SEC-10 Respond to an incident
RCC005: Keep the internal staff, personnel responsible for the management of the STI, third-party personnel involved in operational tasks, and clients informed on the available channels of communication for the receipt of complaints or problems in the process associated with a described scenario.	The policy is disseminated through the internal Amazon communication portal to all employees, vendors, and contractors prior to receiving authorized access to the information system or performing assigned duties.  AWS has developed, documented and disseminated role-based security awareness training for employees responsible for designing, developing, implementing, operating, maintaining, and monitoring the systems managing security and availability and provides resources necessary for employees to fulfill their responsibilities.	OPS-10 Manage workload and operations events



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RCC006: Regarding the audience of the A&T program, the following criteria must be applied:	Considerations	Not applicable.
Characteristics and segmentation of the audience, according to the level of intervention in the process and nature of the function or role that each participant has		
All the necessary participants in the flow must be reached to complete the activity indicated in the scenario.		
Oriented but not limited to: internal staff, personnel responsible for the STI management, suppliers and customers.		
RCC007: With a minimum annual periodicity, an analysis of the A&T program must be carried out to measure the evolution of the incidents, regarding the A&T activities and including as a minimum:		OPS-11 Evolve Operations
Report on the quantity and segmentation of recipients and contents of the A&T program.		
A comparison between the contents covered by the A&T program and the number and type of security incidents reported / detected / known.		



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RCC008: The content of the A&T program must include: measures and techniques for the protection of credentials.		SEC-1 Manage credentials and authentication  SEC-2 Control human access  SEC-3 Control programmatic access
RCC010: The content of the A&T program should include: specific recommendations on security practices on the STI platform.		Not applicable.
RCC012: The content of the A&T program must include specific techniques for the development/acquisition/manufacture, implementation, homologation, and test of security characteristics of the STI, ensuring that the staff involved, internal or external, is properly trained to reduce failures in implementation of security features.		Not applicable.
RCC013: Fls/service providers must have a communication mechanism for the contents of their A&T program that ensures:		OPS-1 Determine priorities
That the recipients are informed continuously.		
That the recipients can make inquiries and clarify any doubts.		



#### **Access Control - Section 7.7.3**

These technical and operational requirements are related to the evaluation, development, and implementation of security measures for the protection of identity, authentication mechanisms, segregation of roles and functions, and other related access features to the outsourced IT services.



#### Requirement **Considerations** RCA049: Fls/service **Shared Responsibility** provider must quarantee AWS customers retain control and ownership of their data and are responsible for that personal data is not managing critical content security requirements. This allows customers to control the accessed, processed or entire lifecycle of their content on AWS and manage their content in accordance with their used by them or any of their own specific needs, including content classification, access control, retention, and suppliers for purposes deletion. different from those AWS gives customers ownership and control over their content by design through tools established in the formal that allow customers to determine where their content will be stored, how it will be agreements of the STI, and secured in transit or at rest, and how access to their AWS environment will be managed. without formal and express AWS has implemented global privacy and data protection best practices in order to help consent of the primary data customers establish, operate, and leverage our security control environment. These controller. security protections and control processes are independently validated by multiple thirdparty independent assessments. AWS has established formal policies and procedures to provide employees a common baseline for information security standards and guidance. The AWS Information Security Management System policy establishes guidelines for protecting the confidentiality, integrity, and availability of customers' systems and content. Maintaining customer trust and confidence is of the utmost importance to AWS.

AWS employees, vendors, and contractors who require a user account must be on-boarded through Amazon's HR management system. As part of the onboarding workflow, the direct manager of the employee, vendor, or contractor requests the establishment of a user account. Group or shared accounts are not permitted within the boundary of the systems that process or store customer data, unless approved for specific business purposes that are in line with certain compliance requirements.

AWS performs a continuous risk assessment process to identify, evaluate, and mitigate risks across the company. The process involves developing and implementing risk treatment plans to mitigate risks as necessary. The AWS risk management team monitors and escalates risks on a continuous basis, performing risk assessments on newly implemented controls at least every six months.

The <u>SOC 2 report</u> provides an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality. More details on the measures AWS puts in place to maintain consistently high levels of security can be found in the <u>Overview of Security Processes Whitepaper</u> AWS Service-Specific Security – page 20.

# Implementation Considerations (Well Architected Practices)

SEC-1 Manage credentials and authentication

SEC-2 Control human access

<u>SEC-3</u> Control programmatic access

SEC-7 Classify data

SEC-8 Protect data at rest



RCA050: Fls/service providers must guarantee the Fl and the BCRA unrestricted access to all documentation and information related to processing, operations and procedures of the STI, when required.

#### **Shared Responsibility**

Customers have full root access or administrative control over accounts, services, and applications and have complete visibility of their cloud resources, services and applications to monitor use and log, collect metrics, set alarms, and automatically react to changes. AWS customers can also provide internal users and regulators logical access to their information and data, if necessary.

Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the SOC 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications, and PCI DSS compliance reports. These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls.

Customers can use <a href="AWS Artifact">AWS Artifact</a>, the automated compliance reporting portal available in the AWS Management Console, to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

There are five AWS SOC Reports all available to AWS customers from AWS Artifact:

- AWS SOC 1 Report
- AWS SOC 2 Security, Availability & Confidentiality Report
- AWS SOC 2 Security, Availability & Confidentiality Report (scope includes Amazon DocumentDB only).
- AWS SOC 2 Privacy Type I Report
- AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.

AWS internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes, but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.

Additionally, BCRA has published regulatory guidance in the form of <a href="Normative">Normative</a> <a href="Interpretations">Interpretations</a>. This guidance has clarified the scope of the BCRA Regulation with respect to FIs' outsourcing to CSPs. In June 2019, BCRA published a Normative Interpretation that acknowledges that the review of international, third-party certifications (such as the ISO certifications) and independent third-party audit reports (such as the SOC reports)

OPS-1 Determine priorities
SEC-1 Manage credentials and authentication



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
	are generally sufficient to satisfy BCRA's and SEFyC's audit and access rights with respect to CSPs providing services to regulated entities. This clarification highlights how these third-party certifications, attestations and audit reports are valuable compliance resources that benefit the FIs and the regulator in their oversight of the outsourced activities. For more information about these third-party certifications and audit reports, see the <a href="AWS Compliance Programs">AWS Compliance Programs</a> webpage.  For more information about AWS approach to access to documentation and information, audit and inspection, and how these requirements may be addressed in an Enterprise Agreement with AWS, please contact your AWS representative.	
RCA051: Fls must ensure that the STI service provider implements and supports the level of controls required for the protection of the services provided, by means of independent measurements, external audits and certifications of international standards.	Shared Responsibility	OPS-1 Determine priorities
	AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding its policies, processes and controls. Customers can leverage this information to perform their control evaluation and verification procedures, as required by the BCRA Regulation and other applicable legislation and regulations.	
	For more information about other AWS certifications and attestations, see the <u>AWS</u> <u>Compliance Programs</u> webpage.	
	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	
	Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards.	
	Customers can use AWS Artifact, the automated compliance reporting portal available in the AWS Management Console, to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.	



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RCA052: Fls/service providers must implement a homogeneous policy of credential management, based on the need for use / know, the separation of incompatible roles, and prevention of collusion, for access to, but not limited to:  Data encryption mechanisms and communication channels.  Privileged users of the operative / applicative platform.  Emergency / contingency users.  Common users.  Fls/service providers must also ensure a life cycle for the access credentials, whose parameters, rules, algorithms, and software involved should be up to date and communicated to the all parties.	Customers retain ownership and control of their content when using AWS services, and do not cede that ownership and control of their content to AWS. Customers have complete control over which services they use and whom they empower to access their content and services, including what credentials will be required.  Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them.  AWS does not change customer configuration settings, as these settings are determined and controlled by the customer. AWS customers have freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture.  AWS provides ways to categorize organizational data based on levels of sensitivity. By using resource tags, AWS IAM policies, AWS KMS, and AWS CloudHSM, customers can define and implement policies for data classification.	SEC-2 Control human access SEC-3 Control programmatic access SEC-7 Classify data SEC-8 Protect data at rest SEC-9 Protect data in transit OPS-1 Determine priorities



#### **Integrity and Registration - Section 7.7.4**

These technical and operational requirements are related to the use of integrity control techniques and data and transaction recording, as well as the handling of sensitive information by STI and techniques that provide traceability and allow its verification. It includes, but is not limited to, transactions, audit records, and validation schemes.

Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RIR003: The records collected for the services provided by the provider must ensure the traceability of the actions carried out in all the activities, identifying who (account, origin, destination), what (activity, function, transaction), where (service, location), when (time), how (pattern, relation of events).	Customer Responsibility AWS offers FI customers tools for governance and data traceability. AWS	OPS-4 Design workload to understand its state
	customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config and AWS Config Rules to track, monitor, analyze, and audit events.	SEC-4 Detect and investigate security events
	AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With AWS CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across AWS infrastructure.	
	AWS CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.	
	Amazon CloudWatch is a resource monitoring & management that gives a complete visibility of cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes.	
	AWS Config is a resource configuration management service that records and evaluates configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis.	



RIR010: The devices/equipment and/or pieces of software arranged by the provider or entity for the STI, must meet a lifecycle and development cycle, based on the following conceptual stages:

- a. Requirements analysis.
- b. Acquisition / manufacture / development.
- c. Test and homologation.
- d. Implementation.
- e. Operation and maintenance.
- f. Decommission and replacement.

Likewise, this cycle must provide the security elements related to, but not limited, to:

- g. Functional safety requirements.
- h. Types and characteristics of validation of the input data.
- i. Granularity of functions and records.
- j. Levels of access.
- k. Change control.
- I. Updates and patches.

#### **Shared Responsibility**

Customers are responsible for managing the entire lifecycle of the devices they own.

AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure quality and security requirements are met with each release.

AWS' strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements.

The design of all new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation.

Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity and availability of the service.

Service reviews are completed as part of the development process.

AWS tracks, documents, and verifies media sanitization and disposal actions. All media removal and disposal is performed by designated AWS personnel.

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their lifecycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

AWS hosts are securely wiped or overwritten prior to provisioning for reuse. AWS media is securely wiped or degaussed and physically destroyed prior to leaving AWS Secure Zones.

To validate AWS' secure wipe processes and procedures, third-party auditors review the guidance within the AWS Media Protection policy, observe degaussing equipment and secure shred bins located within AWS facilities, observe historical tickets which tracked the destruction of a hard

REL-8 Implement change
OPS-6 Mitigate deployment risks

OPS-7 Support a workload



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
	drive within a data center and the process of a device being wiped and removed from the environment.	
	• Data Deletion for block device-based storage (EBS, RDS, ephemeral drives, etc.): In order to ensure that customer content is properly erased, AWS wipes underlying storage media upon reprovisioning rather than upon de-provisioning. Processes that wipe content upon release of an asset (volume, object, etc.) are less reliable than processes that only re-provision clean storage to customers. Physical servers can reboot at any time for many reasons (power outage, system process interruption or failure, etc.), which might leave a wiping procedure in an incomplete state. Customers do not have access to block devices or physical media that was previously used to store another customer's content. For example, in the case of EBS, customers only see their content or zeros (e.g., empty disk) after writing a block or partial block. Wiping blocks at the time storage capacity is re-provisioned is sufficient to ensure that the previous content cannot be recovered from a new volume or object.	
	<ul> <li>Data Deletion for non-block device services: For services such as Amazon S3 or DynamoDB, customers never see an attached block device, only objects and the path to that object (e.g., a table or an item). When a customer deletes an asset in these services, the deletion of the mapping between an asset identifier or key and the underlying content begins immediately. Once the mapping is removed, the content is no longer accessible and cannot be processed by an</li> </ul>	

application.



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RIR011: Fls/service providers must execute a process for the approval of devices/equipment and/or pieces of software to interact with the STI, guaranteeing verification of all aspects of design, functionality, interoperability and security characteristics defined in the acquisition/manufacturing/development stages and implementation.	Customers are responsible for managing the entire lifecycle of the devices they own.  AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure the quality and security requirements are met with each release.  AWS' strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements.  The design of all new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation.  Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity, and availability of the service.  Service reviews are completed as part of the development process.	OPS-1 Determine priorities OPS-5 Reduce defects, ease remediation, and improve flow into production REL-8 Implement change OPS-6 Mitigate deployment risks OPS-7 Support a workload



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RIR020: Fls/service providers must have preventive and corrective mechanisms to attend to requests for access, modification and deletion of personal data, when required to protect the rights of the client.	Customer Responsibility Customers retain ownership and control of their content when using AWS services.  As explained in the Security and Shared Responsibility section, it is important to note that when using AWS services, customers maintain control over their data and are responsible for managing critical content security requirements. This allows customers to control the entire lifecycle of their content on AWS and manage their content in accordance with their own regulatory needs, including to address requests for access, modification, and deletion of personal data by data subjects.  Customers can use the controls available in AWS services, including security configuration controls, for the handling of personal data.  For more information about the Shared Responsibility Model and its implications for the storage and processing of personal data using AWS, see the AWS Whitepaper Using AWS in the Context of Common Privacy and Data Protection Considerations, Data Privacy FAQs website, and our Argentina Data Privacy website, which includes an overview of the Argentina Personal Data Protection Law No. 25,326 (PDPL) and common FAQs.	SEC-1 Manage credentials and authentication SEC-2 Control human access SEC-3 Control programmatic access SEC-7 Classify data SEC-8 Protect data at rest SEC-9 Protect data in transit



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RIR021: Fls/service providers must	Customer Responsibility	REL-9 Back up data
guarantee and establish recovery mechanisms of information assets in the	AWS customers can leverage the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals.	REL-13 Plan for disaster recovery
event of termination and/or indefinite interruption of services and/or relocation, respecting the security	Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment.	
relocation, respecting the security conditions of the information and continuity of operations.	Availability Zones are designed to mitigate against the risk of natural disaster and other disruptions that may occur. Availability Zones are physically separated within a metropolitan region and are in different flood plains. Each Availability Zone is also designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of failure.	
	Customers can achieve extremely high recovery time and recovery point objectives by using multiple Availability Zones and data replication.	
	AWS services allow for the export of content by customers on demand, using the AWS Management Console, APIs, and other input methods. For example, AWS Snowball provides devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud. For more information about migrating data in and out of the AWS Cloud, see <a href="Migration &amp; Transfer on AWS">Migration &amp; Transfer on AWS</a>	



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RIR022: The resources and information used in the STI must be inventoried with their corresponding owner identification and indicating the elimination and validation parameters in the lifecycle of the data.	Customer Responsibility  AWS considers the inventory and lifecycle management of customer data to be an action for Fls to complete.  AWS offers Amazon Macie, a security service that uses machine learning to help customers automatically discover, classify, and protect sensitive data in AWS. This fully managed service continuously monitors data access activity for anomalies and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks, such as access to sensitive data that has accidentally been made externally accessible.  Macie is certified to internationally recognized standards, such as ISO 27017 for cloud security and ISO 27018 for cloud privacy.  AWS provides ways to categorize organizational data based on levels of sensitivity. By using resource tags, IAM policies, AWS KMS, and AWS	SEC-7 Classify data
	CloudHSM, customers can define and implement policies for data classification.	
RIR023: Fls/service providers must establish a life cycle of the registration data of the activities, as established by requirement RIR003, complying with the legal provisions and security provisions for storage, inalterability during the legal time of conservation, and its accessibility to those responsible for control to support forensic investigations in cases of security incidents and detection of security breaches.	Customer Responsibility  AWS offers customers several tools for governance and data traceability.  See our comments to requirement RIR003.	SEC-4 Detect and investigate security events



RIR024: Fls/service providers must establish a data encryption policy for data at rest, in transit or in both states, including the assignment of responsibilities for the controls defined in each state of the data.

### **Customer Responsibility**

Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and what other security features and tools they use and how they use them. AWS is designed to protect the confidentiality and integrity of transmitted data through the comparison of a cryptographic hash of data transmitted. This is done to help ensure that the message is not corrupted or altered in transit. Data that has been corrupted or altered in transit is immediately rejected. AWS provides several methods for customers to securely handle their data:

- Upon initial communication with an AWS-provided Windows Amazon Machine Image (AMI), AWS enables secure communication by configuring terminal services on the instance and generating a unique self-signed X.509 server certificate and delivering the certificate's thumbprint to the user over a trusted channel.
- AWS further enables secure communication with Linux AMIs by configuring Secure Shell (SSH) on the instance, generating a unique host-key and delivering the key's fingerprint to the user over a trusted channel.

Customer Master Keys (CMKs) used for cryptographic operations in AWS Key Management Service (KMS), including operations by AWS employees, are secured by both technical and operational controls. By design, no individual AWS employee can gain access to the physical CMK material in the service due to hardening techniques such as never storing plaintext master keys on persistent disk, using but not persisting them in volatile memory, and limiting which users and systems can connect to service hosts. In addition, multi-party access controls are enforced for operations on the KMS-hardened security appliances that handle plaintext CMKs in memory.

AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]). Additionally, AWS offers customers the ability to add an additional layer of security to data at rest in the cloud, providing scalable and efficient encryption features. It is the responsibility of the AWS customer to enable these features for their systems.

These features include:

SEC-8 Protect data at rest SEC-9 Protect data in transit



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
	<ul> <li>Data encryption capabilities available in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Amazon RDS for Oracle, Amazon RDS for SQL Server, and Amazon Redshift.</li> </ul>	
	<ul> <li>Flexible key management options, including KMS, allow customers to choose whether to have AWS manage the encryption keys or enable customers to keep complete control over their keys.</li> </ul>	
	<ul> <li>AWS customers can employ Server Side Encryption (SSE) with Amazon S3-Managed Keys (SSE-S3), SSE with AWS KMS-Managed Keys (SSE-KMS), or SSE with customer-provided keys (SSE-C).</li> </ul>	
	For more information, see Protecting Data Using Server-Side Encryption.	



RIR025: Fls/service providers must ensure a logical separation of the environments for processing, storage, transport, and recovery of data of the entity from the provider, other entities, and third parties. They must also ensure that the devices/equipment and software that are used or accessed by the environments of the entity should be restricted to those necessary and approved according to requirement RIR011.

### **Shared Responsibility**

Customers are responsible for the separation of the environments and data they create on AWS. Fls must manage access to their content and resources through users, groups, permissions and credentials that customers control.

The <u>Logical Separation Handbook</u> will help FIs understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model.

Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data. Services which provide virtualized operational environments to customers (i.e., EC2) ensure that customers are segregated from one another and prevent cross-tenant privilege escalation and information disclosure via hypervisors and instance isolation.

Different instances running on the same physical machine are isolated from each other via the hypervisor. In addition, the Amazon EC2 firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer; thus, an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical random-access memory (RAM) is separated using similar mechanisms.

Customer instances have no access to physical disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically erases every block of storage before making it available for use, which protects one customer's data from being unintentionally exposed to another. Customers can further protect their data using traditional filesystem encryption mechanisms, or, in the case of Amazon Elastic Block Store (Amazon EBS) volumes, by enabling AWS-managed disk encryption.

A Dedicated Host is also a physical server that's dedicated for customer use. With a Dedicated Host, customers have visibility and control over how hypervised instances are placed on the server. Bare metal instances are non-hypervised host hardware devices. Using the AWS Nitro technology for network and storage offload, as well as the Nitro security chip to eliminate the risks associated with serial single-tenancy on bare metal, customers have direct access to Amazon EC2 hardware. These bare metal instances

SEC-5 Protect networks

REL-2 Network topology

SEC-6 Protect compute resources

OPS-5 Reduce defects, ease remediation, and improve flow into production



R	equirement	Considerations	Implementation Considerations (Well Architected Practices)
		are full-fledged members of the Amazon EC2 service and have access to services such as Amazon VPC and Amazon Elastic Block Store (EBS).	

## **Monitoring and Control - Section 7.7.5**

These requirements define the collection, analysis and control of events in the event of failures, unavailability, intrusions, and other situations that affect the services offered by the providers of STI, and that may generate eventual damage to infrastructure and information.



### Requirement

RMC003: Fls/service providers must follow up with the STI when security settings change and verify the update/patch levels of: operating systems, networks, databases, communication links, prevention and detection tools for malicious code, network security equipment, traffic controllers, and any other security tool. They should include, but not be limited to:

- a. Privilege and access rights tracking;
- b. Copy, backup and information retrieval processes;
- c. Availability of devices / equipment;
- d. Alarms, alerts and problems detected by event management systems.

#### Considerations

### **Shared Responsibility**

Customers are responsible for defining their operational model based on the AWS services they choose to use. Changes to their environments can be detected and tracked using AWS Services such as <a href="AWS Config">AWS Config</a> to assess, audit, and evaluate the configurations of AWS resources.

AWS utilizes a wide variety of automated monitoring systems designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity and alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. Responses are performed according to incident response processes and procedures.

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 Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the <a href="AWS Vulnerability Reporting website">AWS Vulnerability Reporting website</a>.

AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.

# Implementation Considerations (Well Architected Practices)

OPS-4 Design workload to understand its state

<u>SEC-1</u> Manage credentials and authentication

SEC-4 Detect and investigate security events

REL-9 Back up data



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RMC004: Fls/service providers must have transactional monitoring mechanisms in place with the STIs that operate based on profile characteristics and transactional patterns of the client in any of the following action models:	Shared Responsibility See the comments in RMC003.	OPS-4 Design workload to understand its state  SEC-4 Detect and investigate security events
a. Preventive. Detecting, triggering communication actions with the client by alternative ways before confirming operations.		
b. Reactive. Detecting and triggering communication actions with the client after the confirmation of suspect transactions.		
c. Assumed. Detecting and assuming to make the customer whole if the customer claims lack of knowledge of transactions carried out.		
RMC006: From the records collected by the STI resources associated with the scenario, the entities / providers must perform a classification and determination of security events, a definition of limits and thresholds of commitment, levels of normal / unexpected behavior and establish actions according to each classification and limit determined.	Customer Responsibility  Customers are responsible for defining their operational model based on the AWS services they choose to use.  AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config 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.	SEC-4 Detect and investigate security events  SEC-10 Respond to an incident
RMC014: Fls/service providers must determine, document and process the resources, devices/equipment, and software used to monitor STI activities.	Customer Responsibility  Customers are responsible for defining their operational model based on the AWS services they choose to use.	Not applicable.



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RMC015: Fl/service providers must formally establish and execute periodically vulnerability testing and analysis on the resources associated with the STI in all its critical processes.	Customer Responsibility Customers can use AWS services to perform penetration testing and simulated event testing. For more information, see <a href="Penetration Testing">Penetration Testing</a> .	SEC-5 Protect networks SEC-6 Protect compute resources



# **Incident Management - Section 7.7.6**

These technical and operational requirements define the treatment of events and consequent security incidents in the STI, its detection, evaluation, containment, and response, as well as escalation activities and correction of the technical and operational environment.

Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGI001: Fls/service providers must perform with a minimum annual periodicity, and based on the risk analysis of the computer assets associated with the scenario, an analysis of the incidents that have occurred and a report that will serve to establish protection measures, inform the contents of the training and awareness program, modify the registration and control of events, and a redefinition of alerts, limits and thresholds.	Shared Responsibility  AWS considers the development and implementation of mechanisms and plans to detect, respond and manage information security incidents as a shared responsibility between AWS and FIs.  Customers' information security response plans must include the mechanisms for managing all relevant stages of an incident including escalation and reporting. FIs must annually review and test their information security response plans to ensure they remain effective and fit-for-purpose.  AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, 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.  Regarding the AWS incident management process, AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.  The Incident Response Test Plan is executed annually, in conjunction with the Incident Response plan. The test plan includes multiple scenarios, potential vectors of attack, the inclusion of the systems integrator in reporting and coordination (when applicable), and varying reporting/detection avenues (i.e., customer reporting/detecting, AWS reporting/detecting).	SEC-4 Detect and investigate security events SEC-10 Respond to an incident



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RGI002: The identification of incidents must be based at least on early warnings, statistics of type/frequency/pattern of incidents and information security recommendations.	As part of the shared security responsibility model, security events monitoring should be performed by both AWS and FI.  AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, 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, which can be reviewed in the SOC 2 report. Customers can also see all security notifications through AWS Service Health Dashboard or the AWS Personal Health Dashboard.  Monitoring and alarming are configured by AWS to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.  AWS requires that the Security and/or affected Service team conduct a postmortem to determine the cause of incident, as well as to document lessons-learned.	OPS-10 Manage workload and operations events  REL-6 Monitor resources  REL-5 Withstand component failures  PERF-7 Monitor resources to ensure they are performing as expected
RGI003: The management of security incidents can be executed in an outsourced manner but it must be coordinated with personnel of the financial entity.	Shared Responsibility  AWS considers the development and implementation of mechanisms and plans to detect, respond, and manage information security incidents as a shared responsibility between AWS and FIs.  Refer to RGI001/RGI002.	SEC-10 Respond to an incident



RGI005: The detected incidents should receive a regular treatment with an escalation formally defined.

### **Shared Responsibility**

AWS considers the development and implementation of mechanisms and plans to detect, respond, and manage information security incidents as a shared responsibility between AWS and FIs.

Customers information security response plans must include the mechanisms for managing all relevant stages of an incident including escalation and reporting.

AWS customers can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config 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.

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

AWS utilizes a three-phased approach to manage incidents:

- 1. **Activation and Notification Phase:** Incidents for AWS begin with the detection of an event. Events originate from several sources such as:
  - Metrics and alarms AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.
  - Trouble tickets entered by an AWS employee.
  - Calls to the 24x7x365 technical support hotline. If the event meets incident criteria, the relevant on-call support engineer uses the Event Management Tool to start an engagement and page relevant program resolvers (for example, Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.
- . **Recovery Phase** The relevant resolvers will perform break fix to address the incident. After addressing troubleshooting, break fix, and

OPS-10 Manage workload and operations events

SEC-4 Detect and investigate security events

SEC-10 Respond to an incident



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
	affected components, the call leader will assign follow-up documentation and follow-up actions and end the call engagement.	
	2. Reconstitution Phase – The call leader will declare the recovery phase complete after the relevant fix activities have been addressed. The post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and actions, such as design changes. will be captured in a Correction of Errors (COE) document and tracked to completion.	
	To ensure the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverag for the discovery of previously unknown defects and failure modes. In addition, it allows the Amazon Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities.	e



# **Operational Continuity - Section 7.7.7**

These requirements are related to resources and strategic and operational tasks to prevent, contain, and recover critical business processes, financial services, and critical information from failures that affect the availability of STI and the IT infrastructure that supports them.



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RCO001: Must provide the necessary resources for the creation, maintenance, updating, and testing of a data processing continuity plan. The plan must be operational and functional, based on the requirements agreed with the service provider of the outsourced STI, the entity's own requirements, and those regulated by BCRA.	Shared Responsibility Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.  AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic Regions as well as across multiple Availability Zones within each Region. In the case of failure, automated processes move customer data traffic away from the affected area. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains.	REL-9 Back up data REL-5 Withstand component failures REL-12 Test resilience REL-13 Plan for disaster recovery
	Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures, from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover.  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.  In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are	
	redundantly connected to multiple tier-1 transit providers.  Additionally, the AWS Business Continuity plan details the process that AWS follows in the case of an outage, from detection to deactivation. This plan is designed to recover and reconstitute AWS using a three-phased approach: Activation and Notification Phase, Recovery Phase, and Reconstitution Phase. This approach helps AWS perform system recovery and reconstitution efforts in a methodical sequence, aiming to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.  AWS tests the Business Continuity plan and its associated procedures at least annually to ensure effectiveness of the plan and the organization readiness to execute the plan.	



RCO002: Fls/service providers must define, agree, document and implement the methods to determine the impact of an event that disrupts the activities of the entity, the provider or subcontracted third parties including, but not limited to:

- i) Identification of critical resources, including operational and control users;
- ii) Identification of all dependencies, including processes, applications pairs, and subcontracted third parties;
- iii) Detection of threats to critical resources;
- iv) Determination of the impact of planned and non-planned interruptions, and its variation in time:
- v) Establish a maximum tolerable interruption period;
- vi) Establish partial and total recovery periods;
- vii) Establish the maximum tolerable recovery time of critical resources;
- viii) Estimation of resources required for continuity and eventual restoration of operations along with alternate locations.

It should also be given active participation to the primary responsible for the processes and critical resources, guaranteeing full coverage of the STI partners.

### **Shared Responsibility**

See our comments to RCO001.

OPS-4 Design workload to understand its state

OPS-10 Manage workload and operations events

REL-12 Test resilience



Requirement	Considerations	Implementation Considerations (Well Architected Practices)
RCO003: The data processing continuity plan must, consider, but not be limited to, the incorporation of the following content:  a) Manual, logistical and automated emergency operating procedures according to each identified process / resource and determined action;	Shared Responsibility See our comments to RCO001.	REL-9 Back up data REL-5 Withstand component failures REL-12 Test resilience REL-13 Plan for disaster recovery
b) Location, transfer and transport of responsible parties, suppliers and emergency services and physical and logical resources; c) Procedures for recovery / restoration of impacted resources.		
RCO004: The data processing continuity plan must be tested periodically, at least once a year. The tests must be consistent and consistent with the criteria of requirement RCO002. The tests must also ensure that all persons and organizations responsible and participants of the continuity and recovery processes are informed in a regular, continuous and formal way.	Shared Responsibility See our comments to RCO001.	REL-12 Test resilience REL-13 Plan for disaster recovery

