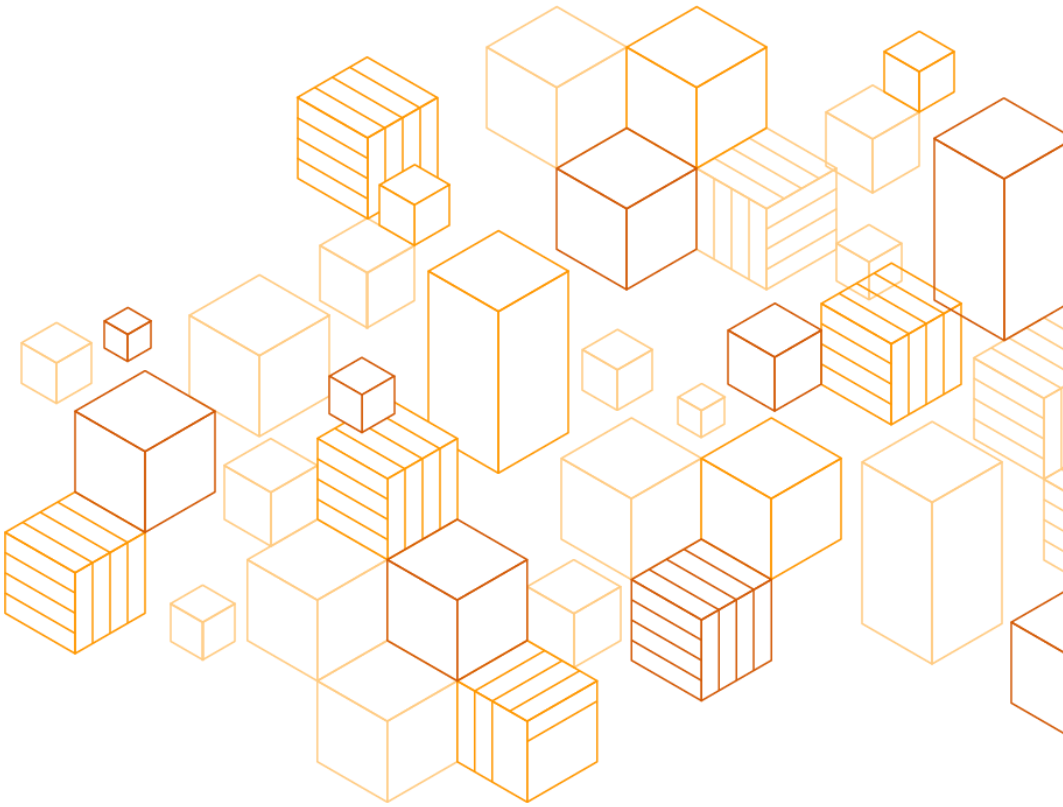
AWS User Guide to Financial Services Regulations in Brazil – Central Bank of Brazil, Resolution 4,893/21 and Resolution 85/21

Updated March 2023

First Published July 2018



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

About this guide

This AWS User Guide to Financial Services Regulations in Brazil provides information to assist financial institutions regulated by the Central Bank of Brazil as they accelerate their use of Amazon Web Services (AWS) cloud services.

This guide provides the following information:

- A Description of the respective roles that financial and payment institutions and AWS each play in managing and securing the cloud environment.
- An Overview of the regulatory requirements and guidance that financial institutions can consider when using AWS.
- Additional resources that financial institutions can use to help them architect and operate their AWS environment to meet regulatory expectations, including under the Central Bank of Brazil's regulations.

Introduction

The National Monetary Council—*Conselho Monetário Nacional* (CMN)—is the main institution responsible for monetary and credit policy within Brazil's financial system. The Central Bank of Brazil—*Banco Central do Brasil* (BCB)—is one of the supervisory authorities linked to CMN responsible for ensuring compliance with the CMN regulations and for the maintenance, regulation, monitoring, and supervision of the financial institutions under its jurisdiction.

On February 26, 2021, BCB issued Resolution No. 4,893 on cybersecurity policy and the requirements for contracting data processing storage and cloud computing services to be complied by financial and other institutions authorized to operate by BCB. In addition, Resolution No. 4,893 revoked and replaced Resolution No. 4,658, issued on April 26, 2018, and Resolution No. 4,752, issued on September 26, 2019.

On April 08, 2021, BCB further issued Resolution No. 85 on cybersecurity policy and the requirements for contracting data processing storage and cloud computing services to be complied by payment institutions. Resolution No. 85 replaced Resolution No. 3,909, issued on August 16, 2018, and Resolution No. 3,969, issued on November 13, 2019.

Resolution No. 4,893 and Resolution No. 85 (together, the BCB Resolutions) articulate and consolidate the steps that financial and payment institutions (Regulated Institutions) are required to take to manage cybersecurity risks in connection with their use of cloud services. The BCB Resolutions require Regulated Institutions to evaluate cloud providers and set up internal controls to manage the relationship with the cloud provider. In so doing, the BCB Resolutions outline a path that Regulated Institutions can follow to use the cloud in a safe and resilient manner.

This guide is intended to be a resource to help Regulated Institutions navigate the requirements of the BCB Resolutions in the context of their cloud adoption. The following sections provide considerations for Regulated Institutions as they assess their responsibilities with regards to the BCB Resolutions. This guide does not cover every provision of the regulations, nor does it address other compliance or legal requirements that may apply to AWS customers. As customers' compliance needs differ, AWS encourages its customers to obtain their own independent assessment on relevant compliance requirements that may be applicable to their business.

Security and the Shared Responsibility Model

Before exploring the specific requirements outlined in the BCB Resolutions, it is important for Regulated Institutions to understand the Shared Responsibility Model. The Shared Responsibility Model is fundamental to understanding the respective roles of customers and AWS in the operation and management of security in the context of the BCB Resolutions.

Compliance and security are a shared responsibility between customer and AWS. AWS manages security *of* the cloud by protecting the infrastructure that runs all of the services offered in the AWS Cloud, including operating, managing and controlling IT components from the host operating system and

virtualization layer down to the physical security of the facilities in which the services operate, while customers are responsible for the security *in* the cloud. This means that customers retain control of the security programs that they choose to implement to protect their content, applications, systems, and networks, as they would for applications in an on-premises data center.

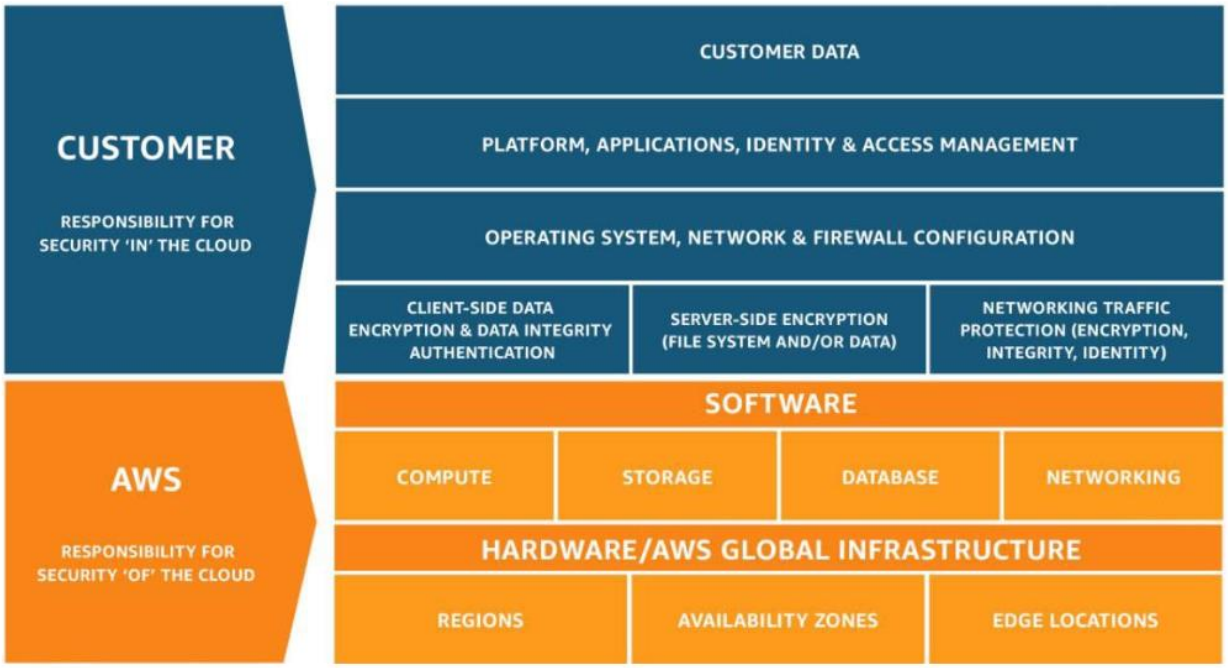


Figure 1: Shared responsibility model

Security *in* the cloud

Customers are responsible for their security in the cloud. AWS customers are responsible for managing the guest operating system, which includes installing updates and security patches and other associated application software, as well as any applicable network security controls.

The customer generally connects to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections; they are part of the customer's area of responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems.

Customers should carefully consider the services they choose because their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It 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 following:

- The content that they choose to store on AWS.
- The AWS services that they use with the content.

- The country where they store their content.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- The way they encrypt their data and where they store their keys.
- 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 is determined by the AWS Cloud services that a customer selects. This selection, in turn, determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as infrastructure as a service (IaaS) and, as such, requires the customer to perform all 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 Identity and Access Management (IAM) tools to apply the appropriate permissions.

Security *of* the cloud

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Customers can use AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following:

- **Validating** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that customers can implement and to better assist customers with managing their control environment.

- **Demonstrating** the AWS compliance posture to help customers 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 Assurance Programs

AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can use the AWS compliance programs to help satisfy their regulatory requirements. For more information about these third-party certifications and audit reports, see 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 particularly important for Regulated Institutions:

ISO 27001 – 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 that defines how AWS perpetually manages security in a holistic, comprehensive manner.

ISO 27017 – ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers.

ISO 27018 – 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 public cloud personally identifiable information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.

ISO 9001 – 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 in which AWS products and services consistently satisfy ISO 9001 quality requirements.

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) or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see PCI DSS Compliance.

SOC – AWS System and 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. 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 and 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. This helps customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications, reports, and attestations, see AWS Compliance Programs. For information about general AWS security controls and service-specific security, see Best Practices for Security, Identity, & Compliance.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports and certifications from accrediting bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

AWS Global Infrastructure

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

AWS customers choose the AWS Regions in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in a location or locations of their choice. More information on our disaster recovery recommendations is available at Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

For example, AWS customers in Brazil can choose to deploy their AWS services exclusively in the South America (São Paulo) Region and store their content onshore in Brazil, if this is their preferred location. If the customer makes this choice, their content will be located in Brazil unless the customer chooses to move that content.

The AWS South America (São Paulo) Region is designed and built to meet rigorous compliance standards globally, providing high levels of security for all AWS customers. As with every AWS Region, the South America (São Paulo) Region is compliant with applicable national and global data protection laws.

The BCB Resolutions

The BCB Resolutions require Regulated Institutions to adopt a cybersecurity policy that addresses a wide range of cybersecurity issues that include the use of service providers for data processing, data storage, and cloud computing.

The BCB Resolutions also require Regulated Institutions to implement and maintain a cybersecurity policy to ensure the confidentiality, integrity, and availability of data consistent with the materiality, size, sensitivity of the data, risk profile, and business model of the services that the Regulated Institution is running in the cloud. The BCB Resolutions identify several features that Regulated Institutions should consider when evaluating a cloud provider.

A full analysis of the BCB Resolutions is beyond the scope of this guide. The following sections focus on some of the key requirements contemplated in the BCB Resolutions and describe how Regulated Institutions can use AWS services to help them meet these requirements.

Implementing a cybersecurity policy

AWS services and the AWS Global Cloud Infrastructure can help Regulated Institutions build secure, high-performing, resilient, and efficient infrastructure for their applications. World-class security experts who monitor AWS infrastructure also build and maintain our broad selection of innovative security services, which can help Regulated Institutions simplify meeting security and regulatory requirements. AWS services are designed to be secure by default. Regulated Institutions can use AWS services and solutions to implement an optimal security posture: Prevent, Detect, Respond, and Recover.

Below are some requirements from the BCB Resolutions framework and information on how Regulated Institutions can use AWS services and solutions to help satisfy the requirements described in the following table.

BCB Resolutions Requirement Summary	AWS Considerations
Chapter II, Section I, article 2 The institution shall implement and maintain a cybersecurity policy based on principles and guidelines designed to ensure confidentiality, integrity, and availability for data and information systems used.	The AWS Cloud infrastructure has been architected to be the most flexible and secure cloud computing environment available. The scale of AWS allows significantly more investment in security policing and countermeasures than almost any large company could afford on its own. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS services, which provide powerful controls to customers. These include security configuration controls for handling sensitive data such as information about financial transactions. AWS helps customers protect against cyber-attacks by providing a number of tools to secure their data. For a list of AWS resources and tools, refer to Security, Identity, and Compliance on AWS. AWS supports TLS/SSL encryption for all its API endpoints and the ability to create VPN tunnels to protect data in transit. AWS also provides the AWS Key Management Service (AWS KMS) and dedicated Hardware Security Module appliances for customers to encrypt data at rest. Customers can choose to secure their data using the AWS provided capabilities or use their own security tools.
Chapter II, Section I, article 3.II The Regulated Institution's cybersecurity policy shall contemplate, among other things, the internal procedures and controls adopted by the Regulated Institution to reduce its vulnerability to incidents and address other cybersecurity objectives.	Customers can use a number of AWS tools to help design secure architectures and reduce their vulnerability to incidents. One key tool is Amazon Inspector, an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available on the Amazon Inspector console or API. Financial institutions can also use AWS services to perform penetration testing and simulated event testing. For more information, see Penetration Testing.
Chapter II, Section I, article 3.III The Regulated Institution's cybersecurity policy shall contemplate, among other things, the specific controls, including those used to ensure data traceability in order to secure sensitive information.	AWS offers customers many tools for governance and data traceability. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. With CloudTrail, customers can log, continuously monitor, and retain account activity related to actions across AWS accounts. CloudTrail provides event history of AWS account activity. This includes 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.

BCB Resolutions Requirement Summary	AWS Considerations
Chapter II, Section I, article 3.V(c) The Regulated Institution's cybersecurity policy shall contemplate, among other things, the guidelines for classifying data and information by its materiality.	AWS provides ways to categorize data based on levels of sensitivity. By using resource tags, IAM policies, and Amazon Macie, customers can define and implement policies for data classification.

This Section Purposely Left Blank

Implementing an action plan and incident response plan

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

Under the Shared Responsibility Model, AWS customers are responsible for establishing and documenting usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access allowed to their systems (including multi-factor authentication) in accordance with their access control policy. AWS customers are responsible for authorizing remote access to their systems prior to allowing such connections.

Regulated Institutions can use tools such as AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, and AWS Security Hub 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 should raise an incident and trigger the incident management process and any appropriate response actions by the Regulated Institution that are necessary to mitigate the incident.

AWS also maintains public notification security bulletins, available in the AWS Security Center. For more details on the measures AWS puts in place to maintain consistently high levels of security, see Best Practices for Security, Identity, & Compliance.

Hiring of cloud computing services

Chapter III of the BCB Resolutions require Regulated Institutions to have risk management policies, strategies, and structures in place that include criteria for using a cloud services provider. The BCB Resolutions set out specific criteria that Regulated Institutions must contemplate in their risk management policies and procedures for using a cloud service provider. The BCB Resolutions specifically state that Regulated Institutions are expected to adopt corporate governance and management practices with respect to outsourcing to service providers proportional to the materiality of the services to be hired and the Regulated Institution's risk exposure.

A Regulated Institution can use AWS services to assist in their compliance with the requirements established in the BCB Resolutions. Some of these requirements are summarized in the following table.

This Section Purposely Left Blank

BCB Resolutions Requirement Summary	AWS Considerations
Chapter III, Article 12 (II) The Regulated Institution's risk management policies and procedures should contemplate the examination of the potential ability of the potential service provider to ensure:	
(a) Compliance with legislation and regulation in force.	AWS customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2, and 3 reports, ISO 27001, 27017, and 27018 certifications, and PCI DSS compliance reports. These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls. Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accrediting bodies across geographies and compliance verticals. AWS internal and external audits are planned and performed according to the documented audit schedule to review the continued performance of AWS against standards-based criteria and to identify general improvement opportunities. Standards-based criteria includes but is not limited to the ISO/IEC 27001, the American Institute of Certified Public Accountants (AICPA): AT 801 (formerly Statement on Standards for Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. For more information about other AWS Compliance Program certifications and attestations, see AWS Compliance Programs.
(b) Access by the Regulated Institution to data and information to be processed or stored by the service provider.	AWS customers retain ownership and control of their data. AWS provides simple, powerful tools that allow customers to determine where their content will be stored, secure the content in transit and at rest, and manage access to AWS services and resources for their users. Customers can do a virtual tour to AWS Datacenters to understand how AWS implements controls, builds automated systems, and undergoes third-party audits to confirm security and compliance. For more information, refer to AWS Cloud Security: our controls.

BCB Resolutions Requirement Summary	AWS Considerations
(c) The confidentiality, integrity, availability, and retrievability of data and information processed or stored by the service provider.	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. The SOC 2 report provides an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
(d) Compliance with certifications required by the Regulated Institution for the provision of services to be hired.	See response to **Chapter III, Article 12(I)(a)**.
(e) The Regulated Institution's access to reports drafted by independent and specialized audit firms hired by the service provider, related to the procedures and controls used to provide the services to be hired.	AWS provides several compliance reports from third-party auditors who have tested and verified its compliance with a variety of information security standards and regulations, including ISO 27001, ISO 27017, and ISO 27018. To provide transparency on the effectiveness of these measures, AWS gives customers options 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.
(f) The provision of information and management resources appropriate to the monitoring of the services to be provided.	Customers can see AWS security notifications via AWS Service Health Dashboard, AWS Security Bulletins, or the AWS Personal Health Dashboard. AWS customers can also use various tools to monitor for abnormalities, such as AWS CloudTrail, Amazon CloudWatch, and AWS Config, including tools available in AWS Marketplace.
(g) Identification and segregation of The Regulated Institution's client data using physical or logical controls. **(h)** Quality of the access controls to protect The Regulated Institution's client data and information.	For more details on the measures AWS puts in place to maintain consistently high levels of security, see Best Practices for Security, Identity, & Compliance. The Logical Separation handbook can help you understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model.

BCB Resolutions Requirement Summary	AWS Considerations
Chapter III, Article 12, 3rd paragraph In the case of running applications over the internet, The Regulated Institution shall ensure that the potential service provider adopts controls to mitigate the effects of any vulnerabilities when new versions of the application are released.	We will be updating the TLS configuration for all AWS service API endpoints to a minimum of version TLS 1.2 by June 2023. For more details, refer to this article on the TLS 1.2 protocol. For customers who require additional layers of network security, AWS offers the Amazon Virtual Private Cloud (VPC), which provides a private subnet within the AWS Cloud and the ability to use an IPsec virtual private network (VPN) device to provide an encrypted tunnel between the Amazon VPC and their data center.
Chapter III, Article 12, 4th paragraph The Regulated Institution shall have the necessary resources and abilities for the appropriate management of the services to be procured, including for the analysis of information and use of resources provided pursuant to Chapter III, Article 12(II)(f) (discussed previously).	AWS Security Fundamentals is a free, self-paced course designed to introduce the fundamentals of cloud computing and AWS security concepts, including AWS access control and management, governance, logging, and encryption methods. It also covers security-related compliance protocols and risk management strategies, as well as procedures related to auditing your AWS security infrastructure. Additional training options can be found at the AWS Training and Certification page.
Chapter III, Article 16 The hiring of material data processing, storage, and cloud computing services provided offshore must comply with the following requirements.	
(I) The existence of an agreement for the exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where services may be provided.	Regulated Institutions are responsible for determining and obtaining the appropriate agreement for exchange of information between the Central Bank of Brazil and the supervisory authorities of countries where AWS services may be provided to them, as required by the BCB Resolutions. For Cloud computing services rendered abroad, customers should review the BCB's list of Memorandums of Understanding (MoU) with different countries published by the Central Bank of Brazil. This list shows the existence of agreements for the exchange of information between BCB and the authorities of the countries where AWS services may be rendered.

BCB Resolutions Requirement Summary	AWS Considerations
(II) The Regulated Institution shall ensure that the provision of the services mentioned above does not cause damage to the regular operation of the Regulated Institution nor hardship to the performance of the BCB.	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 are required. Customers control how they configure their environments and secure their content, including whether they encrypt their content (at rest and in transit), and which other security features and tools they use and how they use them. AWS does not change customer configuration settings because these settings are determined and controlled by the customer. AWS customers have the complete freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how security measures will be implemented in the cloud in accordance with each customer's business needs.
(III) The Regulated Institution shall define, prior to the hiring, the countries and regions in each country where services can be provided and the data may be stored, processed, and managed.	An updated list of AWS services can be found on the AWS site. The AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). AWS Regions provide multiple, physically separated, and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. These Availability Zones offer AWS customers an easier and more effective way to design and operate applications and databases, which makes them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures. The AWS Cloud spans 99 Availability Zones within 31 geographic Regions and more than 410 points of presence (more than 400 Edge Locations and 13 Regional Edge Caches) at the time of publishing this document. For updated information, refer to AWS global cloud infrastructure.
(IV) The Regulated Institution shall establish alternatives for business continuity, in case of impossibility of maintenance or termination of the services agreement.	Please refer to the Business Continuity Plan section of this document.

Agreements with cloud service providers

Chapter III, Article 17 of the BCB Resolutions require Regulated Institutions that use a cloud services provider to have a contractual arrangement in place addressing certain terms. AWS offers a contractual framework that enables customers to comply with the requirements of the BCB.

Business continuity plan

AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance backups, data redundancy replication, and the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS.

The BCB Resolutions require Regulated Institutions to have a business continuity plan that includes certain elements. For example, Chapter III, Section 16(IV) requires a Regulated Institution to establish alternatives for the use of a cloud services provider for business continuity in case of impossibility of maintenance or termination of the services agreement. In addition, Chapter IV, Articles 19 and 20 require Regulated Institutions to have risk management policies that address business continuity and responses to material incidents.

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

AWS maintains a ubiquitous security control environment across all Regions. Regulated Institutions 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. Learn how to architect DR in the AWS Cloud by referring to AWS Elastic Disaster Recovery.

Notification requirement

Chapter III, Article 15 of the BCB Resolutions require Regulated Institutions that hire a cloud service provider to communicate such arrangement to the BCB no later than 10 days after the hiring of the services. The notification must include the corporate name of the service provider, the material services to be hired, and the indication of the countries and regions in each country where services can be provided and data may be stored, processed, and managed.

It is the responsibility of the Regulated Institutions to notify the BCB. Regulated Institutions can use information provided by AWS to help them satisfy this requirement.

This Section Purposely Left Blank

Next steps

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

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best-practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organization throughout your IT lifecycle. The AWS CAF breaks down the complicated process of planning into manageable areas of focus.

Many organizations choose to apply the AWS CAF methodology with a facilitator-led workshop. To find more about such workshops, contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology.

The AWS Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures and provides guidance to help implement designs that scale application needs over time. The Well-Architected framework consists of six pillars:

1. Operational Excellence
2. Security
3. Reliability
4. Performance Efficiency
5. Cost Optimization
6. Sustainability

For Regulated Institutions that are subject to regulations by BCB or CMN in Brazil, next steps also typically include the following:

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

- Consider the relevance and application of the AWS Security whitepapers 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 whitepaper and in the "Additional Resources" section below.
- Speak with your AWS representative to obtain additional information regarding the AWS services agreement.

Additional resources

For additional help visit the Security Learning page, and refer to the following sources:

AWS Artifact

AWS Best Practices for DDoS Resiliency

AWS Security Checklist

CIS AWS Foundations Benchmark

CIS Amazon Web Services Three-tier Web

Amazon Web Services: Risk and Compliance

Document history

Date	Description
July 14, 2021	Reviewed for technical accuracy.
July 2018	First publication.
March 2023	Update.