AWS User Guide to Financial Services Regulations in Brazil – Brazilian National Monetary Council, Resolution 4,658

July 2018

This paper has been archived.

For the latest technical content, see the AWS Whitepapers & Guides page:

https://aws.amazon.com/whitepapers

[Resource Guide]

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. 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

Abstract

This document provides information to assist financial services institutions in Brazil that are regulated by the Brazilian Central Bank as they accelerate their use of Amazon Web Services' cloud services.

Introduction

On April 26, 2018, the Brazilian National Monetary Council, *Conselho Monetário Nacional* ("CMN") issued Resolution No. 4,658 (the "BCB Resolution") establishing cybersecurity requirements for financial institutions ("BFIs") that are regulated by the Brazilian Central Bank, *Banco Central do Brasil* ("BCB"), including requirements for the use of cloud computing services by the BFIs.

The BCB Resolution articulates the steps that BFIs should take to manage cybersecurity risks. It is also the first statement by Brazilian financial regulators about BFIs' use of cloud services. The BCB Resolution requires BFIs to evaluate cloud providers and set up internal controls to manage the cloud provider relationship. In so doing, the BCB Resolution outlines a path that BFIs can follow to use cloud in a safe and resilient manner. AWS welcomes clarity from Brazilian regulators and believes that AWS customers can use AWS services in a manner that is consistent with the Brazilian regulators' security expectations.

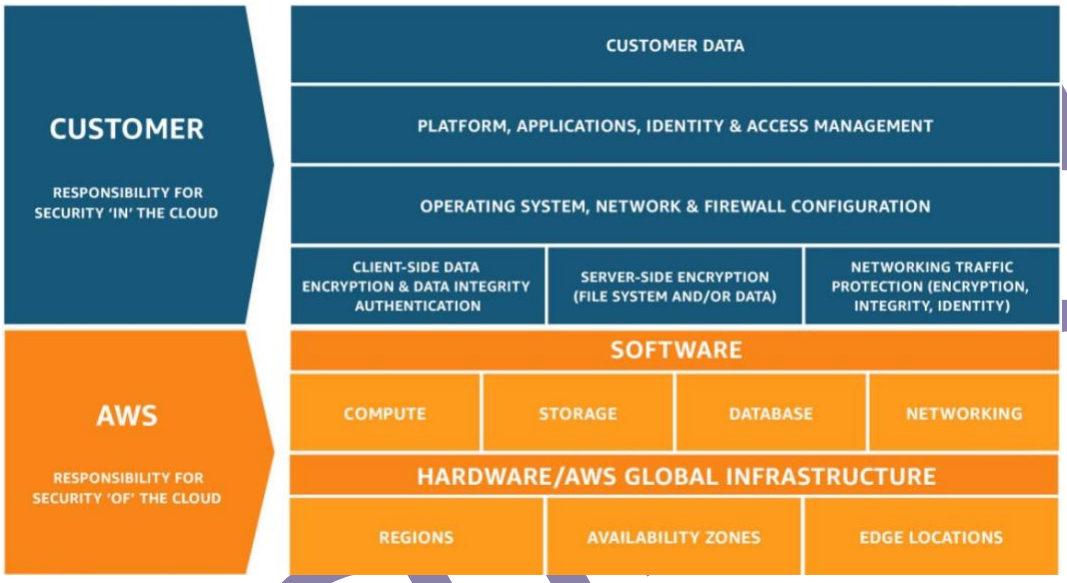
This guide is intended to be a resource to help BFIs navigate the requirements of the BCB Resolution and develop a secure, resilient, and efficient cloud adoption strategy. The following sections provide considerations for BFIs as they assess their responsibilities with regards to the Resolution No. 4,658:

- **Security and Shared Responsibility:** Before exploring the specific requirements contained in the BCB Resolution, it is important that BFIs understand the AWS Shared Responsibility Model. The shared responsibility model is fundamental to understanding the respective roles of the customer and AWS for security and informs the steps BFIs need to take to ensure they comply with the BCB Resolution.
- **AWS Compliance Assurance Programs:** The BCB Resolution requires, among other things, that BFIs perform due diligence on cloud providers. AWS has obtained certifications and third-party attestations for a variety of industry specific workloads. AWS has also developed a security assurance program to make these resources available to customers. Customers can leverage the AWS Security Assurance program to help satisfy their regulatory requirements.
- **AWS Global Cloud Infrastructure:** The AWS Cloud Infrastructure is built around Regions and Availability Zones. The AWS 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 single datacenter infrastructures or multi-datacenter infrastructures. AWS customers can use the AWS Cloud Infrastructure to design an AWS environment consistent with the resiliency requirements of the BCB Resolution.
- **BCB Resolution:** This section sets out common considerations for BFIs that use AWS as they consider some of the key requirements to best suit their regulatory needs.

Taken together, BFIs can use this information to commence their due diligence and assess how to implement an appropriate information security, risk management and governance program for their use of AWS cloud services.

Security and Shared Responsibility

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS 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, platform, applications, systems and networks, no differently than they would for applications in an on-site data center.



Shared Responsibility Model

The Shared Responsibility Model 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. Much like a traditional data center, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided securitygroup firewall. 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. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

Security of the Cloud

In order to provide Security of the Cloud, AWS continuously audits its environments. The infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** 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 can be implemented, and to better assist customers with managing their control environment.
- **Demonstrate** 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.
- **Monitor**, through the use of thousands of security control requirements, that AWS maintains compliance with global standards and best practices.

AWS Compliance Assurance 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 BFIs:

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 which defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001

certification, see the ISO 27001 Compliance webpage.

ISO 27017 – 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 – 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. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.

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 where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the ISO 9001 Compliance webpage.

PCI DSS Level 1 - The Payment Card Industry Data Security Standard (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 – AWS System & Organization Control (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help customers and their auditors understand the AWS controls established to support operations and compliance. For more information, see the SOC Compliance 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; helping

customers to establish and operate in an AWS security control environment.

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

AWS Artifact

Customers can use AWS Artifact 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 Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports and certifications from accreditation bodies across geographies and compliance verticals.

AWS Global Infrastructure

The AWS Cloud infrastructure is built around AWS Regions and Availability Zones. An AWS Region is a physical location in the world that is made up of multiple Availability Zones. Availability Zones consist of one or more discrete data centers that are housed in separate facilities, each with redundant power, networking, and connectivity. These Availability Zones offer customers the ability to operate production applications and databases at higher availability, fault tolerance, and scalability than would be possible from a single data centers. The AWS Cloud operates 55 Availability Zones within 18 AWS Regions around the world. For current information on AWS Regions and Availability Zones, see AWS Global Infrastructure. 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 requirements.

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 on shore 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.

BCB Resolution 4,658

The BCB Resolution requires BFIs to adopt a cybersecurity policy that addresses a wide-range of cybersecurity issues including the use of service providers for data processing, data storage and cloud computing.

If a BFI wishes to use a cloud services provider, the BCB Resolution requires it to adopt a governance model and risk management policies consistent with the materiality of the services that the institution is running in the cloud. The BCB Resolution identifies several features that the financial institution should take into account when evaluating a cloud provider. The BCB Resolution also specifies certain terms that must be included in a contract with a cloud services provider.

A full analysis of the BCB Resolution is beyond the scope of this document. However, the following sections address some of the key requirements contained in the BCB Resolution and describe how BFIs

can leverage AWS services in compliance with these requirements.

Implementing a Cybersecurity Policy

Chapter II, Segment I of the BCB Resolution requires a BFI to adopt and maintain a cybersecurity policy designed to ensure confidentiality, integrity, and availability of data and information systems.

A BFI can use AWS services and the AWS Global Infrastructure to meet the objectives of its cybersecurity policy. AWS Services are designed to be secure by default. BFIs can also leverage AWS to be fully aligned with the NIST Cybersecurity Framework (CSF), and manage security controls to the five risk management functions (Identify, Protect, Detect, Respond, and Recover) and achieve "security in the cloud".

Under the BCB Resolution, a BFI's cybersecurity policy must address certain specific requirements. Some of these requirements, and how AWS can be used to satisfy these requirements are set out below.

BCB Resolution Requirement	**AWS Response**
Chapter II, Segment I, section 2: The BFI 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, including security configuration controls, for the handling of 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. A list of AWS resources and tools is available at: https://aws.amazon.com/products/security/. AWS supports TLS/SSL encryption for all of its API endpoints and the ability to create VPN tunnels to protect data in transit. AWS also provides a Key Management Service and dedicated Hardware Security Module appliances 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, Segment I, section 3.II: The BFI's cybersecurity policy shall contemplate,	Financial institutions can use a number of AWS tools to ensure they have the most secure architecture and reduce their vulnerability to incidents. One key tool is Amazon Inspector. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It automatically assesses applications for vulnerabilities or deviations

among other things, the internal procedures and controls adopted by the BFI to reduce its vulnerability to incidents and address other cybersecurity objectives	from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API. Financial institution customers can also use AWS services to perform penetration testing and simulated event testing. For more information, please visit https://aws.amazon.com/pt/security/penetration-testing/
Chapter II, Segment I, section 3.III: The BFI'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 financial institutions 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 infrastructure. CloudTrail provides event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.
Chapter II, Segment I, section 3.V(c) The BFI's cybersecurity policy shall contemplate, among other things, the guidelines for classifying data and information by its materiality	AWS provides ways to categorize organizational data based on levels of sensitivity. By using resource tags, IAM policies, AWS KMS, and AWS CloudHSM, customers can define and implement policies for data classification.

Implementing an Action Plan and Incident Response Plan

Chapter II, Segment III of the BCB Resolution requires a BFI to have in place cybersecurity action plans and incident response procedures.

AWS has implemented a formal, documented incident response policy and program. This information can be reviewed in AWS's SOC 2 report, which is available to customers under a non-disclosure agreement. For more information, please see the "AWS Artifact" session.

In addition, 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. Information about how to handle incident response in the cloud is available at this blog post.

AWS also maintains public notification security bulletins, available in the AWS Security Center. More

details on the measures AWS puts in place to maintain consistently high levels of security can be found in the AWS Overview of Security Processes Whitepaper, available in PT-BR.

Hiring of Cloud Computing Services

Chapter III of the BCB Resolution requires BFIs to have risk management policies, strategies, and structures in place that include criteria for using a cloud services provider. The BCB Resolution sets out specific criteria that BFIs' risk management policies and procedures for using a cloud service provider contemplate. The BCB Resolution specifically states that BFIs 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 BFI's risk exposure.

A BFI can use AWS to meet all of these requirements for cloud service providers in the BCB Resolution. Some of these requirements, and how AWS can help BFI customers meet these requirements are set out in the chart below.

BCB Resolution Requirement	AWS Response
Chapter III, Section 12.II A BFI'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 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 legislation and regulations. For more information about other AWS certifications and attestations, see the AWS Assurance Program webpage.
(b) Access by the BFI 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. Please visit https://aws.amazon.com/pt/compliance/data-center/data-centers/
(c) The confidentiality, integrity, availability, and retrievability of data and information processed or stored by the service provider	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 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 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 BFI for the provision of the service to hired	See response to Chapter III, Section 12.I(a), above.
(e) The BFI'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 computer 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 all of AWS's security notifications via AWS Service Health Dashboard or the AWS Personal Health Dashboard. AWS customers can also use various tools to monitor for abnormalities, such as AWS CloudTrail, Amazon CloudWatch, AWS Config and AWS Config Rules, including tools available in AWS Marketplace.
(g) Identification and segregation of the BFI's client data using physical or logical controls (h) Quality of the access controls to protect the BFI's client data and information	More details on the measures AWS puts in place to maintain consistently high levels of security can be found in PT-BR AWS Overview of Security Processes Whitepaper, AWS Service-Specific Security – page 20. The Logical Separation Handbook will help you understand logical separation in the cloud and demonstrates its advantages over a traditional physical separation model.
Chapter III, Section 12 § 3 In the case of running applications over the internet, the BFI shall ensure that the potential service provider adopts controls to mitigate the effects of any vulnerabilities when new versions of the application are released	Customers can connect to an AWS access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. For customers that 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, Section 12 § 4 The BFI shall have the necessary resources and abilities to the appropriate management of the services to be hired, including for the analysis of information and use of resources provided pursuant to Chapter III, Section 12.II(f) (discussed above)	A BFI can use AWS resources to make sure that its personnel have the appropriate training and resources to manage AWS services. 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 https://aws.amazon.com/pt/training/.
Chapter III, Section 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 Brazilian Central Bank and the supervisory authorities of the countries where services may be provided;	For Cloud computing services rendered abroad, customers should review the BCB's list of Memorandums of Understanding (MoU) with different countries published by the Brazilian Central Bank, and available at http://www.bcb.gov.br/fis/supervisao/memsupervisao.asp?idpai=SUPERVISAOSFN. 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.
II. The BFI shall ensure that the provision of the services mentioned above does not cause damage to the regular operation of the institution, nor embarrassment 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 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 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 BFI 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 at https://aws.amazon.com/pt/. 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, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures. The AWS Cloud spans 55 Availability Zones within 18 geographic Regions and one Local Region around the world, the updated information is available at https://aws.amazon.com/pt/about-aws/global-infrastructure/.
The financial institution shall establish alternatives for the business continuity, in case of impossibility of maintenance or termination of the services agreement	See response in the "Business Continuity Plan" section below.

Agreements with Cloud Service Providers

Chapter III, Section 17 of the BCB Resolution requires BFIs that use a cloud services provider to have a contractual arrangement in place that includes certain terms.

BFIs have the option to enroll in an Enterprise Agreement with AWS. These agreements give customers the ability to tailor their agreements to best suit their needs, including any regulatory requirements. Through an AWS Enterprise Agreement, AWS is able to offer BFIs an agreement that contains the relevant terms required by Chapter III, Section 17 of the BCB Resolution.

Business Continuity Plan

The BCB Resolution requires BFIs to have a business continuity plan that includes certain elements. For example, Chapter III, Section 16.IV requires the BFI 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, Sections 19 and 20 require a BFI 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. 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. Customers can learn how to architect DR in the AWS Cloud here: https://aws.amazon.com/pt/disaster-recovery/.

Notification requirement

Chapter III, Section 15 of the BCB Resolution requires BFIs that hire a cloud service provider to communicate such arrangement to the BCB at least 60 days prior to 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.

AWS considers the BFI's notification to the BCB as an action for the BFI to independently complete, but the BFI can leverage information provided by AWS to satisfy its requirement.

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 will enable staff to thrive in the cloud.

The AWS Cloud Adoption Framework (AWS CAF) offers structure to help organizations develop an efficient and effective plan for their cloud adoption journey. Guidance and best-practices prescribed within the framework can help you build a comprehensive approach to cloud computing across your organization, throughout your IT lifecycle. The AWS CAF 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, please contact your AWS representative. Alternatively, AWS provides access to tools and resources for self-service application of the AWS CAF methodology at https://aws.amazon.com/professional- services/CAF/.

For BFIs in Brazil, next steps typically also 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 at https://aws.amazon.com/pt/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 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 "Further Reading" section below.
- Speak with your AWS representative to obtain additional information regarding the AWS Enterprise Agreement.

Further Reading

For additional help visit the AWS Security Whitepapers, and see 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
- Securing Data at Rest with Encryption
- AWS Best Practices for DDoS Resiliency
- Cloud Adoption Framework - Security Perspective
- Introduction to AWS Security Processes
- AWS Security Best Practices
- Encrypting Data at Rest
- AWS Risk & Compliance
- Using AWS in the Context of Common Privacy and Data Protection Considerations
- Security at Scale: Logging in AWS
- Security at Scale: Governance in AWS
- Secure Content Delivery with CloudFront