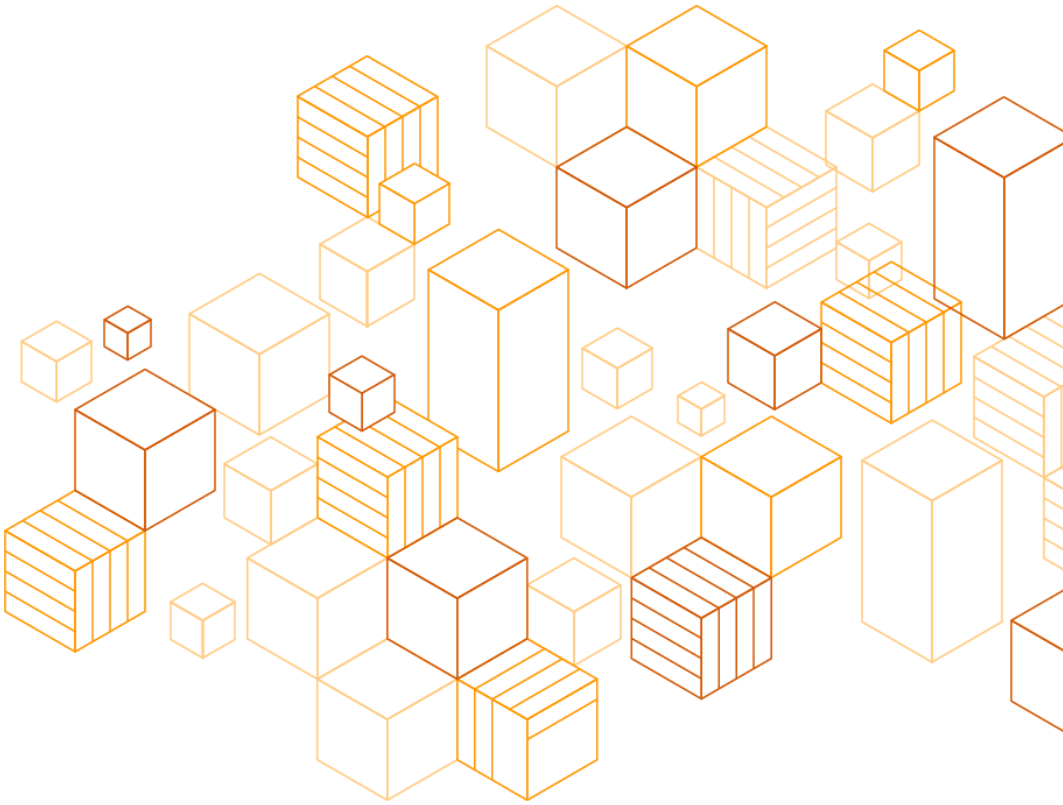
# AWS User Guide to Regulations Applicable to Credit Institutions in Mexico

**National Banking and Securities Commission (CNBV): General Rules Applicable to Credit Institutions**

***December 18, 2021***



# 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 document provides information to assist Credit Institutions[1] in Mexico regulated by the National Banking and Securities Commission (Comisión Nacional Bancaria y de Valores or "CNBV") 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.
- Describes AWS's security systems and shared responsibility model.
- Provides an overview of the regulatory requirements set forth in the General Rules Applicable to Credit Institutions (Circular Única de Bancos or "CUB").
- Provides additional resources to assist Credit Institutions design and architect their AWS environment to meet their security and regulatory objectives.

[1] Unless otherwise indicated, all references to "Credit Institutions" shall refer to "Instituciones de Crédito" as defined by the Circular Única de Bancos and Article 2 of Ley de Instituciones de Crédito.

# Overview

AWS provides secure and resilient global cloud infrastructure services to financial services institutions across banking, global payments, capital, and insurance markets. Across the world, financial institutions (FIs) use AWS services to modernize and automate their core applications, including mobile banking, regulatory reporting, and market analysis. Through continuous innovation, AWS is able to provide strong security systems, the greatest breadth and depth of services in the industry, deep industry expertise, and an expansive partner network to FIs globally. AWS empowers FIs to modernize their technology 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.

The CNBV is Mexico's primary regulatory agency in charge of regulating and overseeing the use of cloud services by Credit Institutions. The CNBV possesses regulatory authority over a broad set of FIs in Mexico, including brokerage and exchange houses, credit unions, financial technology institutions ("Fintechs"), community and rural financial corporations, deposit warehouses, foreign exchange firms, and credit unions, among others. The specific regulatory requirements applicable to FIs, including those related to the outsourcing of technology services, vary depending on the classification of the FI and the applicable regulatory authority and regulation. This document focuses on Credit Institutions.

In December 2005, the CNBV issued the CUB to compile the rules applicable to Credit Institutions regulated by the CNBV. The CUB includes specific contractual, operational, and technical requirements with which regulated Credit Institutions must comply when outsourcing Information Technology ("IT") services to cloud service providers ("CSPs").

This document is a resource to help Credit Institutions understand the technical and operational requirements that may apply to them under the CUB when they use AWS. This document also describes the AWS compliance framework and advanced tools and security measures which Credit Institutions may find helpful for evaluating and demonstrating their compliance with the applicable regulatory requirements under the CUB.

A full analysis of the CUB is beyond the scope of this guide. However, the sections outlined below address the primary considerations that recurrently arise in our interactions with Credit Institutions in Mexico and provide information that such institutions can use to help them understand their and AWS's responsibilities under the CUB.

- **Security and Shared Responsibility**: It is important that Credit Institutions understand the AWS Shared Responsibility Model before evaluating the specific technical and operational requirements outlined in the CUB. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS with respect to security and information access.

- **AWS Compliance Programs:** AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. AWS has also developed compliance programs to make these resources available to customers. Customers can 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 help them design an AWS environment consistent with their business and regulatory needs, including applicable requirements under the CUB.
- **Considerations on the Circular Única de Bancos (CUB)**: This section sets out common considerations for Credit Institutions that use AWS as they consider some of the key technical and operational requirements under the CUB and describes how Credit Institutions can leverage AWS services and tools to help them comply with their regulatory requirements. A list of requirements and corresponding considerations is provided in the Appendix: AWS Considerations on Operational and Security Requirements in the CUB.

# Security and AWS Shared Responsibility Model

It is important that Credit Institutions understand the AWS Shared Responsibility Model before navigating their operational and technical requirements under the CUB. 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. Namely, our 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.

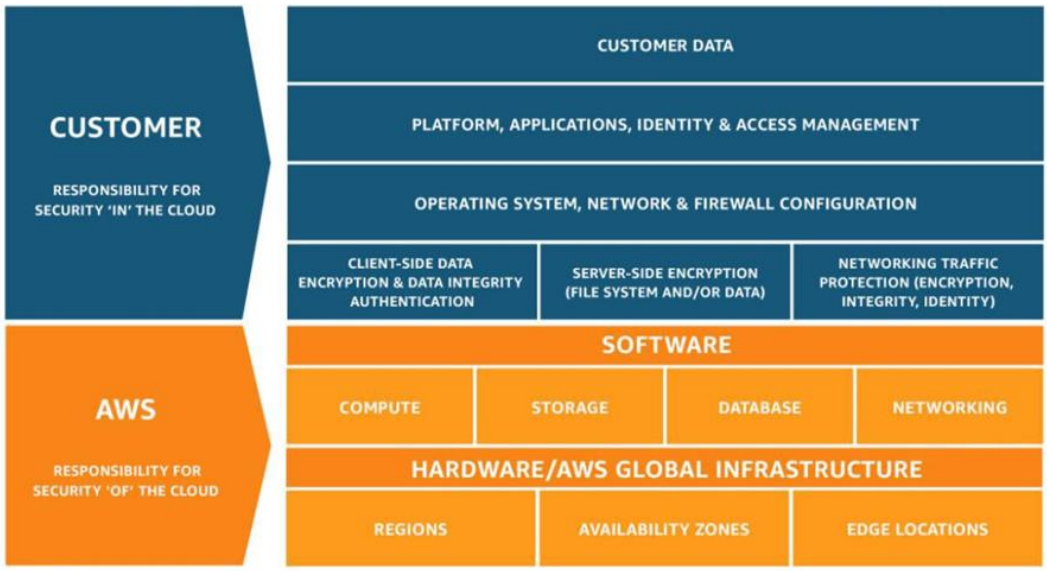



*Figure 1: Shared Responsibility Model*

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security. 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 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.
- How 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'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:

- **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 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 banks and Credit Institutions:

**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** 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 CSPs. 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 ISO 27018 Compliance 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 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 -** 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 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.

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

## AWS Artifact

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 SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

# AWS Global Infrastructure

The AWS Global Cloud infrastructure 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 Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond.

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 Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

# Considerations on the Circular Única De Bancos

## Outsourcing by Financial Institutions

The CNBV allows Credit Institutions to outsource Information Technology ("IT") services to third-party Cloud Services Providers ("CSPs") operating in Mexico or abroad. The CUB imposes specific requirements on Credit Institutions that decide to outsource IT services to CSPs that operate outside of Mexico.

Under the CUB, Credit Institutions must seek authorization from the CNBV when outsourcing IT services to third-party CSPs operating abroad and must comply with certain technical and operational requirements.

### A. Authorization Requirement

The general requirements with which Credit Institutions must comply to outsource IT services to third-party CSPs are found in Articles 318[2] and 328 of the CUB. Under Article 328, banks and Credit Institutions must request authorization from the CNBV at least twenty (20) business days before contracting the services of a third-party CSP operating abroad.[3] Among other requirements, this request must include documentation that demonstrates compliance with certain technical and contractual requirements. The CNBV must respond to the applicable Credit Institution within twenty (20) business days after the application has been submitted, as stipulated in Articles 328 and 326.[4] Under the CUB, the request is considered approved by default if such Credit Institution does not receive a written response from the CNBV within the twenty (20) days stipulated above, and they can start using the services of the third-party CSP.

[2] Unless otherwise indicated, all "Article" references in this document are to the CUB as of the publication date of this document.

[3] The CNBV published a guide that Credit Institutions may follow to seek authorization from the CNBV: Guía Para La Autorización De Contratación Con Terceros De Servicios o Comisiones.

[4] Credit Institutions should be mindful that the authorization process can take longer. The twenty (20) day response period from the CNBV is automatically and indefinitely extended if the CNBV responds with additional questions or requests.

For more information regarding these requirements, see AWS Considerations on Operational and Security Requirements in the CUB. As part of the authorization requirements set forth above, Credit Institutions must comply with the contractual requirements described in Article 318. Credit Institutions that are AWS customers have the option to enroll in an AWS Enterprise Agreement with AWS.

AWS Enterprise Agreements give customers the option to have tailored agreements that best suit their needs, including regulatory requirements generally applicable to FIs.

Through an AWS Enterprise Agreement, AWS can offer Credit Institutions regulated by the CNBV a contractual framework that helps them satisfy the applicable contractual requirements under the CUB, including specific terms that address the CNBV's access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative. If you do not have an AWS representative, please contact us.

### B. Data Privacy

Credit Institutions should also evaluate and consider the application of data privacy laws in Mexico. Although the CUB does not add specific data privacy requirements that apply when outsourcing IT services to foreign CSPs, Article 328 requires Credit Institutions to contract with third-party CSPs that reside in jurisdictions whose laws provide protections to personal data.[5]

### C. Post-Approval Compliance

Once a Credit Institution has obtained approval from the CNBV to outsource IT services to a CSP, such Credit Institution must ensure continuous compliance with the technical and operational requirements described in the CUB including in Article 316 Bis 11, the security and information processing requirements in Article 316 Bis 10, and the access control requirements in Article 316 Bis 11. For more information, please see the appendix below: AWS Considerations on Operational and Security Requirements in the CUB.

## Support Plans

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

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

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

[5] The AWS whitepaper, Using AWS in the Context of Common Privacy and Data Protection Considerations provides useful information to customers using AWS cloud services to store or process personal data.

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

# Getting Started

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

For Credit Institutions in Mexico, next steps typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, and AWS Solution Architects, Professional Services teams, and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, please contact us.
- Obtain and review a copy of the latest AWS SOC 1 & 2 reports, PCI-DSS Attestation of Compliance and Responsibility Summary, and ISO 27001 certification from AWS Artifact (accessible via the AWS Management Console).
- Consider the relevance and application of the AWS Security Whitepapers, AWS Well-Architected Framework, 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 below.
- Speak with your AWS representative to obtain additional information regarding the AWS Enterprise Agreement and determine the support level that matches your needs.

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

# Additional Resources

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

- AWS Compliance Quick Reference Guide: AWS has many features to assist you in meeting compliance objectives 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.
- The Amazon Web Services (AWS) Security Reference Architecture (AWS SRA) is a holistic set of guidelines for deploying the full complement of AWS security services in a multi-account environment. It can be used to help design, implement, and manage AWS security services so that they align with AWS best practices. The recommendations are built around a single-page architecture that includes AWS security services—how they help achieve security objectives, where they can be best deployed and managed in your AWS accounts, and how they interact with other security services. This overall architectural guidance complements detailed, service-specific recommendations such as those found on the AWS Security website.
- 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: AWS Operational Excellence Pillar; AWS Security Pillar; AWS Reliability Pillar; AWS Performance Efficiency Pillar; AWS Cost Optimization Pillar.
- Global Financial Services Regulatory Principles: AWS has identified five common principles related to financial services regulation that customers should consider when using AWS Cloud services and specifically, applying the Shared Responsibility Model to their regulatory requirements. Customers can access a whitepaper on these principles at AWS Artifact.

- NIST Cybersecurity Framework (CSF): The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (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). Credit Institutions 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 |
|---|---|
| **Dec. 18, 2021** | First publication |

# Appendix: AWS Considerations on Operational and Security Requirements in the CUB.

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

The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—the Well-Architected 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:

- **Requirements Summary:** This column summarizes the requirements in the CUB.
- **Considerations:** This column explains considerations for addressing the requirements defined in the CUB. It may refer to the security and compliance of the cloud, and how AWS implements and manages controls and/or AWS services that Credit Institutions can use to help them address these requirements.
- **Implementation Considerations:** This column lists best practices for security in the cloud from the AWS Well-Architected Framework that Credit Institutions 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 for their applicable requirements under the CUB. 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.

## Third Section - Using Third Parties to Carry out Operational Processes or Administration of Databases and Computer Systems

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 326**<br>Credit Institutions hiring third parties for database and computer systems administration must give notice to the CNBV prior to the use of services.<br>Notice to CNBV must specify the databases or computer systems in question and be delivered to the CNBV at least twenty (20) business days in advance of the contract date. | **Customer Responsibility**<br>Credit Institutions are required to notify the CNBV when outsourcing information technology services to a third-party CSP. However, as part of this notification, Article 328 also requires that Credit Institutions obtain authorization from the CNBV before using the services of a foreign CSP such as AWS. Article 328 is discussed in more detail below. | Not applicable. |
| **Article 327.**<br>The notice referenced in Article 326 must be signed by the Director General of the Credit Institution and meet the following requirements:<br>**I.** Contain the report referenced in section II of Article 318 and, if the services provided include information technology and telecommunications, an additional technical report that specifies the services to be carried out in compliance with Annex 52.<br>**II.** Attach the draft contract for the provision of services. | **Customer Responsibility**<br>Credit Institutions in Mexico must provide to the CNBV a technical report that specifies the type of operations or banking services to be carried out by the applicable third-party CSP. Furthermore, Credit Institutions must show in the aforementioned report the manner in which they will comply with the minimum operating and security guidelines set forth in Annex 52. | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 328.**<br>Credit Institutions require authorization of the CNBV for using the services of third parties provided or executed partially or completely outside of Mexico.<br>Credit Institutions must request authorization at least (20) twenty business days before contracting with the third party and document compliance with requirements in Article 318. | **Customer Responsibility**<br>Credit Institutions in Mexico are required to obtain authorization from the CNBV before outsourcing information technology services to CSPs that operate outside Mexico, such as AWS. The CNBV requires Credit Institutions to request authorization at least twenty (20) days before contracting with the relevant CSP.<br>The authorization request must contain the proper documentation described in Articles 328 and 318 (discussed below). | Not applicable. |
| **Article 328 – I.**<br>Documentation must be provided to prove that the third-party resides in countries whose laws protect personal data, safeguard due confidentiality, or have international agreements with Mexico on that matter. | **Customer Responsibility**<br>The AWS customer can choose the AWS Region or Regions in which their content will be located and can choose to deploy their AWS services exclusively in a single Region if preferred.<br>AWS services are structured so that a customer maintains effective control of customer content regardless of what Region they use for their content. This allows customers to establish environments that meet specific geographic or regulatory requirements. | Not applicable. |
| **Article 328 – II.**<br>Credit Institutions will maintain in offices in Mexico documentation related to evaluations, results of audits, and performance reports. When the CNBV requires it, they must provide such documentation in Spanish. | **Customer Responsibility**<br>AWS Customers can use AWS Artifact, the automated compliance reporting portal available in the AWS Management Console, to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies. Restrictions may apply to the translation of reports and other documentation available through AWS Artifact.<br>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. | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 328 – III.**<br>Provide proof that the Board, the Audit Committee, or the Risk Committee approved:<br>**a)** Use of the services does not place the Credit Institution at risk of not fulfilling its obligations.<br>**b)** Business practices of the third party are consistent with those of the Credit Institution.<br>**c)** No impact on financial stability or operational continuity of the Credit Institution due to this contract.<br>**d)** The measures to be implemented in the cases in section VII of Article 318. | **Customer Responsibility**<br>AWS customers are responsible for defining their operational process model for managing systems, databases, and services, as well as the risk assessment process they use.<br>As an AWS customer, you maintain ownership of your content, and you select which AWS services can process, store, and host your content. AWS does not access or use your content for any purpose without your consent. AWS never uses customer content or derive information from it for marketing or advertising.<br>The requirements described in Article 326 are discussed above. | Not applicable. |
| For the request of authorization, the provisions of the penultimate and last paragraphs of Article 326, and Article 327, shall apply.<br>The CNBV will have the power to require the Credit Institution to provide draft and final contracts translated to Spanish. | | Not applicable. |

## Chapter XI – Third Party Contracts / First Section – General Provisions

**Article 318**: Credit Institutions, with the exceptions provided in sections I to XXVII of Article 317, must comply with the following requirements to hire any of the services referred to in this chapter.

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **I.** Not applicable. | Not applicable. | Not applicable. |
| **II.** Maintain a report that lists computer systems and operational processes subject to the services, as well as the criteria and procedures used to select the third party. | **Customer Responsibility**<br>AWS customers are responsible for defining their operational process model for managing systems, databases, and services, as well as the risk assessment process they use.<br>To help AWS Customers get the most from the AWS security control framework, AWS has developed a security assurance program that uses best practices in global privacy and data protection.<br>The AWS Compliance Programs help customers to understand the robust controls in place at AWS to maintain security and compliance in the cloud.<br>AWS provides a consistent approach for AWS customers to evaluate architectures, and provides guidance that can help customers implement designs. | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **III.** Include in the service contract with the third party service provider, their acceptance of, among others: certain confidentiality obligations; obligation to report changes to its business purpose; and audits by the Credit Institution and by the CNBV. | **Shared Responsibility**<br>Through an AWS Enterprise Agreement, AWS offers Credit Institutions regulated by the CNBV a contractual framework that may help them satisfy the applicable contractual requirements under the CUB, including specific terms that address the CNBV's access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative. | Not applicable. |
| **IV.** Establish guidelines and mechanisms to avoid affecting the adequate provision of the Credit Institution's services to the public, its financial stability, or operational continuity after ending the contract with the service provider; including the verification that the service provider does not keep any information about the Institution or its customers afterwards. | **Customer Responsibility**<br>Customers retain ownership and control of their content and its lifecycle when using AWS services, and do not cede that ownership and control of their content to AWS. 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.<br>AWS services allow for the export of content by customers on demand, using the AWS Management Console, APIs, and other input methods. For example, AWS Snowball provides devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud. For more information about migrating data in and out of AWS, see: Migration & Transfer on AWS. The AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation. | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **V.** Ensure compliance to the minimal security and operations provisions on Annexes 52 and 58. | **Customer Responsibility**<br>Customers are responsible for defining their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use. AWS supports customers building their architecture based on regulatory and customer requirements.<br>As explained in the "Security and Shared Responsibility" section, cloud security is a shared responsibility. AWS manages security of the cloud, ensuring that AWS infrastructure complies with global regulatory requirements as well as best practices.<br>However, security in the cloud is the responsibility of the customer. This means that customers are responsible for the security programs they deploy to protect their content, platform, applications, systems, and networks in the same way as they do in a local data center.<br>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.<br>AWS supports AWS Customers' authorization process with CNBV, providing technical support, information and documentation for the AWS Compliance Programs.<br><br>Annex 52 is further explained on Page 22. | OPS 4 Design for workload insights<br>OPS 7 Operational readiness<br>OPS 8 Workload health<br>OPS 10 Event response<br>SEC 1 Secure Operations<br>SEC 4 Security events<br>SEC 7 Data classification<br>SEC 8 Data protection at rest<br>SEC 9 Data protection in transit<br>SEC 10 Incident response<br>REL 4 Design interactions to prevent failures<br>REL 5 Design interactions to mitigate failures<br>REL 6 Resource monitoring<br>REL 9 Data backup<br>REL 10 Fault isolation<br>REL 11 Resiliency implementation<br>REL 12 Reliability testing<br>REL 13 Disaster recovery<br>PERF 7 Monitor performance |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **VI.** Verify that the service provider, is not included in lists of persons linked to resources of illicit origin, terrorism or its financing, or other illegal activities; whether published by Mexican authorities, international organisms, intergovernmental organizations, or authorities in other countries . | **Customer Responsibility**<br>Customer should document that they confirmed AWS was not part of these lists at the moment of the contracting. Additional guidance on lists can be found on the CNBV site. | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **VII.** Establish criteria to assess the extent to which contracting the services could impact the Credit Institution's operations, considering the following:<br>**a)** The capacity of the Credit Institution to maintain operational continuity.<br>**b)** The complexity and time required to find a replacement for the third party providing services.<br>**c)** The ability of the Credit Institution to maintain appropriate internal controls in case of suspension of the service by the third party.<br>**d)** The impact that the suspension of the service would have on the finances, reputation, and operations of the Credit Institution.<br>**e)** The vulnerability of customer information. | **Customer Responsibility**<br>AWS customers can leverage the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals. Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment. Using multiple Regions further increases resiliency.<br>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.<br>The most resilient architectures use multiple AWS Regions. AWS Regions provide greater geographic separation than using a single Region. AWS Regions are designed to be autonomous, with dedicated copies of services deployed in each Region. AWS customers can use multiple Regions to operate workloads that require high availability and mitigate the risks of large-scale physical disruptions.<br>AWS services allow for the export of content by customers on demand, using the AWS Management Console, APIs, and other input methods. For example, AWS Snowball provides devices designed to be secure to transfer large amounts of data into and out of the AWS Cloud. For more information about migrating data in and out of AWS, see: Migration & Transfer on AWS.<br>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.<br>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.<br>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. | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Art. 318 Bis**<br>Information requests and corrective actions identified by the Commission will be addressed directly to the Credit Institution. The Commission is entitled to perform visits and audits as defined on Article 318.<br><br>**Art. 318 Bis I**<br>The Credit Institution must perform audits every two years to verify regulatory compliance of the services being provided, including the infrastructure, controls, and operations of the service provider's site. | **Shared Responsibility**<br><br>Through an AWS Enterprise Agreement, AWS offers Credit Institutions regulated by the CNBV a contractual framework that may help them satisfy the applicable contractual requirements under the CUB, including specific terms that address the CNBV's access and inspection rights. For more information about AWS Enterprise Agreements, please contact your AWS representative.<br><br>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.<br><br>Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.<br><br>There are four AWS SOC Reports all available to AWS customers from AWS Artifact:<br>• AWS SOC 1 Report<br>• AWS SOC 2 Security, Availability & Confidentiality Report<br>• AWS SOC 2 Privacy Type I Report<br>• AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.<br><br>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. | Not applicable. |

| **Annex 52 - Minimum Operating and Safety Guidelines for Using Technological Support Service**<br>**Requirements Summary** | **Considerations** | **Implementation Considerations**<br>**(Well Architected Practices)** |
|---|---|---|
| **I. Operational Requirements.**<br>**a.** Redundancy mechanisms to minimize risk of interruption.<br>**b.** Continuity strategy to operate during failures.<br>**c.** Monitor quality of service and system response times.<br>**d.** Technical support to solve problems.<br>**e.** Mechanisms that will allow the Institution to keep under its protection, either in its own Technological Infrastructure or that of third parties, in both cases in national territory, the detailed records of all the Operations carried out, as well as accounting records in such a way that ensures operational continuity at all times.<br>**II. Security Requirements.**<br>**a.** Sensitive Information is encrypted.<br>**b.** Establishment of duties of the Security Officer.<br>**c.** Log access to information.<br>**III. Audit and Supervision.**<br>**a.** Policies and procedures to carry out audits every two years.<br>**b.** Access to the technological environment from the Institution's facilities in Mexico. | **Customer Responsibility**<br>Customers define their governance, risk assessment, and operational model, and can do so based on the AWS services and products they use.<br>As explained in the "Security and Shared Responsibility" section, cloud security is a shared responsibility. AWS manages security of the cloud, ensuring that AWS infrastructure complies with global regulatory requirements as well as best practices.<br>However, security in the cloud is the responsibility of the customer. This means that customers are responsible for the security programs they deploy to protect their content, platform, applications, systems, and networks in the same way as they do in a local data center.<br>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.<br>AWS supports AWS Customers' authorization process with CNBV, providing technical support, information and documentation for the AWS Compliance Programs.<br>Additional information is available at: Guía para la autorización de contratación con terceros de servicios o comisiones on the web portal of the Mexican government.<br>Customers can define the workload's architecture to meet specific geographic or regulatory requirements. Customers can work with AWS account manager and AWS architect for assistance on architecture definition. | OPS 4 Design for workload insights<br>OPS 7 Operational readiness<br>OPS 8 Workload health<br>OPS 10 Event response<br>SEC 1 Secure Operations<br>SEC 4 Security events<br>SEC 7 Data classification<br>SEC 8 Data protection at rest<br>SEC 9 Data protection in transit<br>SEC 10 Incident response<br>REL 4 Design interactions to prevent failures<br>REL 5 Design interactions to mitigate failures<br>REL 6 Resource monitoring<br>REL 9 Data backup<br>REL 10 Fault isolation<br>REL 11 Resiliency implementation<br>REL 12 Reliability testing<br>REL 13 Disaster recovery<br>PERF 7 Monitor performance |

## Fifth Title - Other Dispositions - Chapter X - Use of Electronic Banking Services

## Fourth Section - Security, Confidentiality, and Integrity of Information Transmitted, Stored or Processed Via Electronic Media

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 316 Bis 10.**<br>Credit Institutions must implement security measures for transmission, storage, and processing of information:<br>**I.** Use encrypted channels to transmit Sensitive Information.<br>**II.** Encrypt information related to accounts or operations of their Users and encrypt any Authentication Factor.<br>**III.** Never transmit unencrypted Passwords and PINs.<br>**IV.** Ensure that cryptographic keys and Encryption and Decryption processes are deployed on high-security devices, such as HSM (Hardware Security Module)**.**<br>**V.** If debit and credit cards are used:<br>**a)** Obtain certifications of security standards of the card industry, including, among others: PCI-DSS, PA-DSS, PTS or their equivalents. | **Customer Responsibility**<br>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.<br>AWS protects 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.<br>AWS CloudHSM is a service for creating and managing cloud-based hardware security modules. A hardware security module (HSM) is a specialized security device that generates and stores cryptographic keys. If you need to secure your encryption keys in a service backed by FIPS-validated HSMs, but you do not need to manage the HSM, you may consider AWS Key Management Service.<br>For the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.<br>For more information, visit S3 User Guide - Protecting Data Using Server-Side Encryption. | SEC 7 Data classification<br>SEC 8 Data protection at rest<br>SEC 9 Data protection in transit<br>PERF 5 Networking selection |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 316 Bis 11.**<br>Credit Institutions must have controls for access to databases and files.<br>Credit Institutions must comply with:<br>**I.** Access to databases and files is provided only on a case by case basis and only for authorized personnel.<br>**II.** Remote access must use encryption mechanisms.<br>**III.** Have safe destruction procedures for storage media.<br>**IV.** Policies for information use and storage. Verify compliance by suppliers. | **Shared Responsibility**<br>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.<br>In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user and programmatic access to AWS services and resources. You can apply granular policies, which assign permissions to a user, group, role, or resource. You also have the ability to require strong password practices, such as complexity level, avoiding re-use, and enforcing multi-factor authentication (MFA). You can use federation with your existing directory service. For workloads that require systems to have access to AWS, IAM enables secure access through roles, instance profiles, identity federation, and temporary credentials.<br>AWS has no insight as to what type of content the customer chooses to store in AWS and the customer retains complete control of how they choose to classify their content and where it is stored, used, and protected from disclosure.<br>AWS provides an advanced set of access, encryption, and logging features such as AWS CloudTrail to help FIs do this effectively. We do not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users.<br>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, by providing scalable and efficient encryption features. It is the responsibility of the AWS customer to enable these features for their systems.<br>In order to ensure asset management inventory and maintenance procedures are properly executed, AWS assets are assigned an owner, and are tracked and monitored with AWS proprietary inventory management tools.<br>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.<br>AWS tracks, documents, and verifies media sanitization and disposal actions. All media removal and disposal is performed by designated AWS personnel. | SEC 2 Authentication<br>SEC 3 Authorization and access control |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| | Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycle. We have 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.<br>AWS is audited by external auditors on more than 2,600 requirements throughout the year. When third-party auditors inspect our data centers they do a deep dive to confirm we are following established rules needed to obtain our security certifications, which includes media decommissions. To know more about these controls see: AWS Data Center Controls. | |

## Fifth Section – Monitoring, Control, and Business Continuity for Electronic Banking Services

| Requirement Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 316 Bis 13.**<br>Credit Institutions must maintain mechanisms for the detection and prevention of events that deviate from habitual use by their users.<br>For such purposes, Credit Institutions may:<br>**I.** Request from users information necessary to define their habitual use of services.<br>**II.** Apply prevention measures. | **Shared Responsibility**<br>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 AWS Config to assess, audit, and evaluate the configurations of AWS resources.<br>AWS customers can configure logging throughout the workload, including application logs, resource logs, and AWS service logs. For example, ensure that AWS CloudTrail, Amazon CloudWatch Logs, Amazon GuardDuty and AWS Security Hub are enabled for all accounts within your organization.<br>AWS customers can use automation to investigate and remediate events to reduce human effort and error, which can enable them to scale investigation capabilities. Regular reviews will help you tune automation tools, and continuously iterate. For example, automate responses to events by automating the first investigation step, then iterate to gradually remove human effort using Amazon GuardDuty, a continuous security monitoring service that helps you to identify unexpected and potentially unauthorized or malicious activity in your AWS environment.<br>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.<br>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.<br>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 | SEC 4 Security events<br>SEC 5 Network protection<br>SEC 6 Compute protection<br>REL 6 Resource monitoring<br>OPS 8 Workload health<br>OPS 9 Operations health |

| Requirement Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| | that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities.<br>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 AWS Vulnerability Reporting website. | |
| **Article 316 Bis 14.**<br>Credit Institutions must maintain databases with information on the operations carried out through the electronic banking service which are challenged by customers for at least five years following the registration of the information. | **Customer Responsibility**<br>Customers retain ownership and control of their content and its lifecycle when using AWS services, and do not cede that ownership and control of their content to AWS. 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. | REL 6 Resource monitoring<br>REL 9 Data backup<br>SEC 10 Incident response<br>OPS 4 Design for workload insights |
| **Article 316 Bis 19**<br>Credit Institutions must ensure continuous operation of the technology infrastructure, as well as promptly restore electronic banking services after incidents.<br>Incidents must be reported to the Audit and Risk committees to adopt appropriate measures to prevent their re-occurrence. | **Customer Responsibility**<br>AWS customers can leverage the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals.<br>Customers may choose to use multiple Regions to operate workloads that require high availability. Customers can also mitigate the risks of large-scale physical disruptions by using multiple Regions. AWS Regions are designed to be autonomous, with dedicated copies of services deployed in each Region. The most resilient architectures use multiple AWS Regions.<br>Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment. 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.<br>Customers can achieve extremely high recovery time and recovery point objectives by using multiple Availability Zones and data replication.<br>Customers can learn more about these topics by downloading: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond, and Disaster Recovery of Workloads on AWS: Recovery in the Cloud. | OPS 1 Operations priorities<br>OPS 4 Design for workload insights<br>OPS 8 Workload health<br>OPS 9 Operations health<br>REL 6 Resource monitoring<br>REL 9 Data backup<br>REL 10 Fault isolation<br>REL 11 Resiliency implementation<br>REL 12 Reliability testing<br>REL 13 Disaster recovery<br>PERF 7 Monitor performance |

| Requirement Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Article 316 Bis 21**<br>Credit Institutions must implement corrective actions that the CNBV requires as a result of the identification of risks associated with the use of electronic banking services. | **Shared Responsibility**<br>Customers are responsible for defining their operational model based on the AWS services.<br>On the AWS side of the Shared Responsibility Model, 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.<br>AWS regularly reviews and remediates issues in order to address non-conformities. The following information is identified for any issue that impacts AWS's control environment:<br>• Details of issue identified<br>• Root cause<br>• Compensating controls<br>• Severity<br>• Owner<br>• Near term path forward<br>• Long term path forward<br>Depending on the nature and severity of the non-conformity, records of the corrective actions taken may be reviewed during a regularly scheduled AWS Leadership team meeting. | OPS 4 Design for workload insights<br>OPS 8 Workload health<br>OPS 9 Operations health<br>OPS 10 Event response<br>OPS 11 Operations evolution<br>SEC 4 Security events<br>SEC 10 Incident response<br>PERF 7 Monitor performance |
| **Article 316 Bis 22**<br>In the event of natural catastrophes affecting banking operations and services, the CNBV may authorize Credit Institutions to provide electronic banking services under different terms until conditions return to normal. | **Customer Responsibility**<br>AWS customers can leverage the features of the AWS infrastructure and AWS services to meet a wide range of resiliency goals.<br>Using multiple Availability Zones, even within a single Region, can enhance resiliency as compared to an on-premises environment. Using multiple Regions further increases resiliency.<br>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 Zones is also designed as an independent failure zone and automated processes move customer traffic away from the affected area in the case of failure. | Not applicable. |

| Requirement Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| | Customers can achieve extremely high recovery time and recovery point objectives by using multiple Availability Zones and data replication.<br>The most resilient architectures use multiple AWS Regions. AWS Regions provide greater geographic separation than using a single Region. AWS Regions are designed to be autonomous, with dedicated copies of services deployed in each Region.<br>AWS customers can use multiple Regions to operate workloads that require high availability.<br>AWS customers can also mitigate the risks of large-scale physical disruptions by using multiple Regions.<br>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, please see: Migration & Transfer on AWS. | |

# Second Title – Prudential Provisions - Chapter VI - Internal Controls

## Sixth Section General Management

| Requirement | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Articles 164. IV, f, and 164 Bis.**<br>General Management must protect integrity of technology infrastructure and confidentiality of data as per guidelines in Article 168 Bis 11.<br>General Management must prepare the Business Continuity Plan observing the provisions of Annex 67.<br>Director(s) will be responsible for:<br>**I.** Implementation, continuous updating, and dissemination of the plan within the Credit Institution.<br>**II.** Design and execution of a communication policy regarding contingency verification.<br>**III.** Make the CNBV aware of operating contingencies. | **Shared Responsibility**<br>Customers are responsible for properly implementing contingency planning, training and testing for their systems hosted on AWS.<br>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.<br>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.<br>Customers can also utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site.<br>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.<br>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.<br>In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AWS Availability Zones 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.<br>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. | Not applicable. |

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.

Additionally, as part of the shared security responsibility model, security events monitoring should be performed by both AWS and AWS customers.

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

Customers can learn more about these topics by downloading: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond, and Disaster Recovery of Workloads on AWS: Recovery in the Cloud.

## ANNEX 67 – Minimum Requirements for Business Continuity Plan

| Requirement | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **Credit Institutions, prior to the development of a Business Continuity Plan, must carry out a business impact analysis that:**<br>**a)** Identifies critical processes for continuity of operations.<br>**b)** Determines resources needed to maintain and restore services.<br>**c)** Defines relevant scenarios such as:<br>**i.** Disasters.<br>**ii.** Infectious diseases.<br>**iii.** Cyber-attacks.<br>**iv.** Sabotage.<br>**v.** Terrorism.<br>**vi.** Interruptions in power supply.<br>**vii.** Failures of tech infrastructure.<br>**viii.** Unavailability of tech resources.<br>**ix.** Interruptions in services provided by third parties.<br>**d)** Estimates quantitative and qualitative impacts of scenarios.<br>**e)** Defines recovery priorities.<br>**f)** Determines Recovery Time Objective.<br>**g)** Establishes recovery objective point.<br>**h)** Identifies and evaluates risks related to processes and services. | **Shared Responsibility**<br>Customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS.<br>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.<br>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.<br>Customers can utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site.<br>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.<br>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.<br>In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AWS Availability Zones 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.<br>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.<br>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. | OPS 1 Operations priorities<br>OPS 2 Operating model<br>REL 10 Fault isolation<br>REL 13 Disaster recovery |

| Requirement | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **i)** Determines risks of location of data processing centers. | 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.<br>Additionally, as part of the shared security responsibility model, security events monitoring should be performed by both AWS and AWS customers.<br>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.<br>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 the AWS Personal Health Dashboard.<br>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.<br>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.<br>Customers can learn more about these topics by downloading: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond, and Disaster Recovery of Workloads on AWS: Recovery in the Cloud. | |
| **II. The Business Continuity Plan, must incorporate the following strategies:**<br>**a) Prevention.**<br>**i.** Reduce vulnerability of the Credit Institution.<br>**ii.** Provision of human, financial, material infrastructure as necessary.<br>**iii.** Establishment of a program to test the Plan. | **Shared Responsibility**<br>Customers are responsible for properly implementing contingency planning, training, and testing for their systems hosted on AWS.<br>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.<br>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 11 Resiliency implementation<br>REL 12 Reliability testing<br>OPS 11 Operations evolution |

| Requirement | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| **iv.** Training program referred to in section I of Article 164 bis.<br>**v.** Communication policy referred to in section II of Article 164.<br>**vi.** Procedures for registration, monitoring, and dissemination of findings.<br>**b) Contingency.**<br>**i.** Identify in a timely manner the nature of the Operational Contingencies.<br>**ii.** Contain the effects of Operational Contingencies on critical processes.<br>**c) Restoration**.<br>**d) Evaluation**. | Customers can utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site.<br>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.<br>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.<br>In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, AWS Availability Zones 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.<br>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.<br>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.<br>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.<br>Additionally, as part of the shared security responsibility model, security events monitoring should be performed by both AWS and AWS customers.<br>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.<br>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 the AWS Personal Health Dashboard. | |

| Requirement | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| | 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.<br>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.<br>Customers can learn more about these topics by downloading: Amazon Web Services' Approach to Operational Resilience in the Financial Sector & Beyond, and Disaster Recovery of Workloads on AWS: Recovery in the Cloud | |
| Credit Institutions, when defining the different actions and procedures, must at all times clearly determine the responsible personnel, as well as foresee personnel replacement. | **Customer Responsibility**<br>AWS Customers are responsible to define Roles and Responsibilities (R&R) for their processes. | Not applicable. |

## Eighth Section BIS – Information Security

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| Credit Institutions must protect integrity and availability of technology infrastructure and confidentiality of data. | **Shared Responsibility**<br>See our response to Article 168 Bis 11 below. | Not applicable. |
| **Article 168 Bis 11.**<br>The Director(s) of the Credit Institution will be responsible for the implementation of the internal control system regarding Information Security that ensures confidentiality, integrity, and availability. | **Shared Responsibility**<br>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.<br>Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, including Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.<br>There are four AWS SOC Reports all available to AWS customers from AWS Artifact:<br>• AWS SOC 1 Report<br>• AWS SOC 2 Security, Availability & Confidentiality Report<br>• AWS SOC 2 Privacy Type I Report<br>• AWS SOC 3 Security, Availability & Confidentiality Report, publicly available as a whitepaper.<br>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 | Not applicable. |

| Requirements Summary | Considerations | Implementation Considerations (Well Architected Practices) |
|---|---|---|
| | Attestation Engagements (SSAE) 16), and the International Standards for Assurance Engagements No.3402 (ISAE 3402) professional standards. | |
| **Art. 168 Bis 16.**<br>**I.** Provide the necessary information to make the CNBV aware of Information Security Incidents.<br>**II.** Conduct an immediate investigation and send results to the CNBV within 15 business days after the Incident. | **Customer Responsibility**<br>AWS Customers are responsible for complying with these requirements from the CNBV regarding Information Security incidents. | Not applicable. |
| **Article 168 Bis 17.**<br>Credit Institutions will keep records of Information Security incidents for at least 10 years. | **Customer Responsibility**<br>AWS Customers are responsible for complying with these requirements from the CNBV regarding Information Security incidents. | Not applicable. |