AWS Mexico Compliance Guide

December 2024

Notices

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

Contents

Overview 5

Privacy 5

Public cloud procurement framework (Contrato Marco) 6

Security and compliance in AWS 8

AWS security and shared responsibility 9

Security in the cloud 10

Security of the cloud 10

AWS Global Cloud Infrastructure 12

Sustainability in Mexico 12

Achieving emissions reductions 13

Reducing water usage in AWS data centers 13

AWS compliance programs 15

Methods to prove compliance with the privacy laws 18

Steps to use the public cloud procurement framework 23

Additional resources 24

Getting started 26

Contributors 27

Document revisions 27

Abstract

This document provides guidance to assist both private and public sector organizations (agencies and entities) in Mexico as they adopt and accelerate their use of the AWS Cloud.

This guide covers the requirements for two specific categories of regulations, privacy and procurement.

Privacy:

- Describes key aspects of National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP), which applies to individuals or legal entities of the private sector.
- Describes key aspects of INAI's General Law on Protection of Personal Data Held by Obligated Parties (LGPDPPSO), which regulates the processing of personal data by the public sector.
- Provides comments and implementation considerations to help customers subject to these regulations map AWS controls to the requirements and guidelines of the LFPDPPP and LGPDPPSO.

Procurement:

- Details the key components of the Secretariat of Public Office (SFP) public cloud procurement framework (Contrato Marco Servicios de Nube Pública Bajo Demanda).
- Outlines the procedures that public sector organizations must adhere to when implementing the procurement framework.

This document provides a sample of controls, but not an exhaustive list. It is not intended as legal or compliance advice. Customers should consult their own legal and compliance teams.

For clients from the Financial Sector, AWS also provides extensive resources on Mexico's AWS Compliance Center webpage.

Overview

Amazon Web Services (AWS) provides Mexico organizations with the secure, resilient, global cloud infrastructure and services they need to differentiate themselves today and adapt to the needs of tomorrow. Through continuous innovation, AWS delivers stringent security requirements, the greatest breadth and depth of services, deep industry expertise, and an expansive partner network. Building on AWS empowers organizations to modernize their infrastructure, meet rapidly changing customer requirements and expectations, and drive business growth. AWS offers IT services in categories ranging from compute, storage, database, and networking to AI and machine learning. Across the world, high-security organizations have used AWS services to build their own applications for engineering, system development, and operational support.

Privacy

The Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) was published in July 2010 and regulates the processing of personal data (defined as any information concerning an identified or identifiable natural person) carried out by individuals or legal entities of the private sector. Subsequently, the Congress of the Union approved various regulations that regulate data privacy, including the General Law on Protection of Personal Data Held by Obligated Parties (LGPDPPSO), which regulates the processing of personal data by the public sector. The National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) is the autonomous constitutional body of Mexico responsible for verifying compliance with both laws and their regulations.

In the case of the private sector, Article 52 of the LFPDPPP states that personal data controllers can use services, applications and infrastructure in the cloud as long as the cloud provider complies with certain requirements related to, among other things, the protection of privacy for personal data. For the public sector, this same authorization is found in Article 63 of the LGPDPPSO.

AWS cares about your privacy and the security of your data. At AWS, security starts with our core infrastructure. Designed specifically for the cloud and to meet the world's most stringent security requirements, our infrastructure is monitored 24/7 to protect the confidentiality, integrity, and availability of our customers' data. The same world-renowned security experts who oversee this infrastructure also create and maintain our wide selection of innovative security services, which can help you meet your own security and regulatory demands. As an AWS customer, regardless of your size or location, you

have the benefits of our expertise, which is measured against the most stringent third-party security programs.

AWS implements and maintains technical and organizational security measures applicable to AWS cloud infrastructure services under globally recognized security certifications and regulatory frameworks, including ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 14001, PCI DSS Level 1, and SOC 1, 2 and 3. These technical and organizational security measures are validated by independent third-party assessors and are designed to prevent unauthorized access or disclosure of customer content.

For example, ISO 27018 is the first international code of practice that focuses on the protection of personal data in the cloud. It is based on the ISO 27002 information security standard and provides application guidelines on ISO 27002 controls applicable to personally identifiable information (PII) processed by public cloud service providers. This certification demonstrates to customers that AWS has a system of controls specifically geared toward protecting the privacy of their content.

The technical and organizational security measures of AWS are consistent with the requirements of the LFPDPPP and the LGPDPPSO to protect personal data. Customers using AWS services maintain control over their content and are responsible for implementing additional security measures based on their specific needs, including content classification, encryption, access management and security credentials.

Because AWS does not have visibility into the type of content customers choose to store on AWS, including whether or not that content is considered subject to the LFPDPPP and the LGPDPPSO, customers are ultimately responsible for their own compliance. The content of this guide supplements existing data privacy resources to help you align your requirements with the AWS Shared Responsibility Model when processing personal data in AWS.

Public cloud procurement framework (Contrato Marco)

In 2024, Mexico's Secretariat of Finance and Public Credit (SHCP), in collaboration with the Coordination of the National Digital Strategy (CEDN), released the country's first public cloud procurement framework called *Contrato Marco Servicios de Nube Pública Bajo Demanda*.

This procurement framework allows public sector institutions and entities—as defined in Article 2 of the Public Sector Procurement, Leasing, and Services Law (LAASSP)—to

contract cloud services derived from the framework without being subject to the standard public bidding procedure, as indicated in section XX of Article 41 of the LAASSP.

AWS and its partners listed in the procurement framework meet the specific technical, legal, and administrative requirements set by the SHCP, and public sector institutions and entities can purchase AWS Services listed on the Contrato Marco's Annex 1 Technical Annex.

Security and compliance in AWS

The following sections clarify the responsibilities of AWS and address the controls that AWS customers can use to address security requirements under their responsibility.

- Security and shared responsibility: It is important that organizations understand that security and compliance are a shared responsibility between AWS and the customer, before exploring the specific requirements of regulations. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS for security and informs the steps organizations need to take to support compliance.
- AWS Global Cloud Infrastructure: The AWS Global Cloud Infrastructure comprises AWS Regions and Availability Zones and offers AWS customers a straightforward and more effective way to design and operate applications and services, making them more highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use the AWS Global Cloud Infrastructure to design an AWS environment consistent with their business and regulatory needs.
- AWS Compliance Program: 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. Organizations can use AWS compliance programs to help satisfy their regulatory requirements.

AWS security and shared responsibility

The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles, and it is important that organizations understand the model before exploring the specific regulatory requirements.

Customers are responsible for security *in the cloud*. What this means is that customers retain control of the security program they choose to implement to protect their own content, applications, systems, and networks, as they would for applications in an on-premises data center.

AWS manages security *of the cloud* by verifying that the AWS Cloud Infrastructure aligns with global and regional regulatory requirements and best practices. 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.

The Shared Responsibility Model is represented graphically in Figure 1.

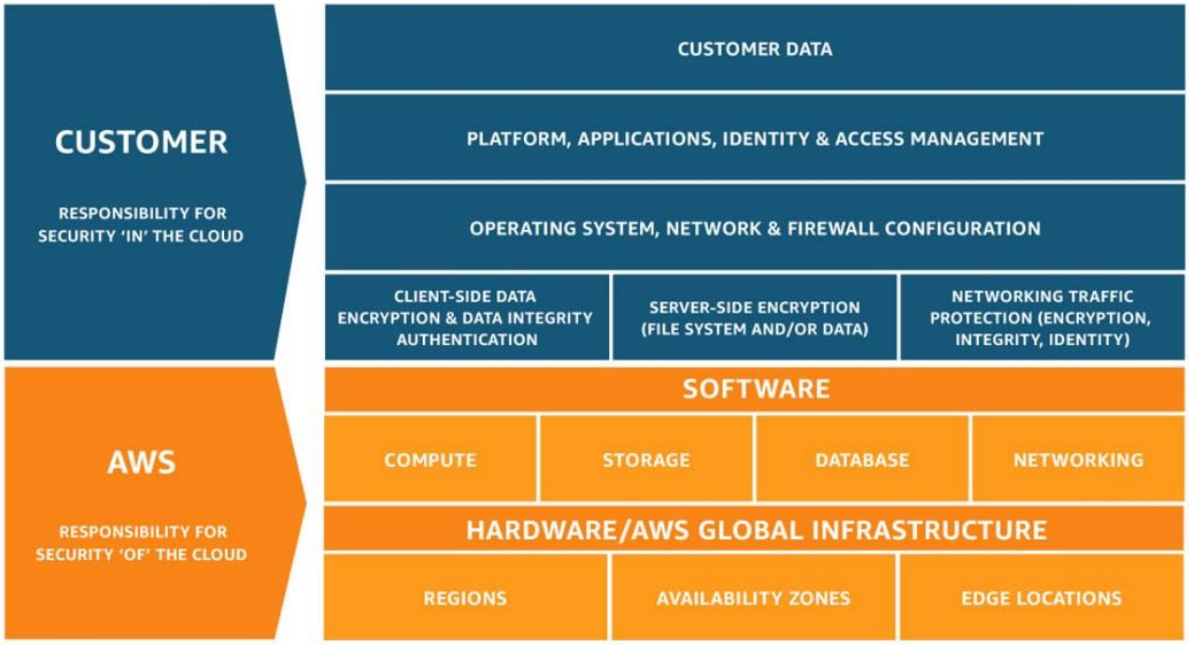

Figure 1: Shared Responsibility Model

Security in the cloud

Customers are responsible for *security in the cloud*. Customers should carefully consider the services they choose, because their responsibilities vary depending on the services that 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.
- AWS services that are used to store the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility is determined by the AWS cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) requires the customer to perform all the necessary security configuration and management tasks of a general-purpose computer. Customers that deploy an 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 customers access service 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 tools to enforce the appropriate permissions.

Security of the cloud

AWS infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can

use compliance certifications held by AWS 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:

- **Validation** that AWS services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. The AWS control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud services 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 alignment 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 alignment with global standards and best practices.

AWS Global Cloud Infrastructure

AWS Global Cloud Infrastructure spans 108 Availability Zones within 34 geographic regions, with announced plans for 18 more Availability Zones and six more AWS Regions in Mexico, New Zealand, the Kingdom of Saudi Arabia, Thailand, Taiwan, and the AWS European Sovereign Cloud.

AWS offers a broad set of global cloud-based products including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, Internet of Things (IoT), security, and enterprise applications: on-demand, available in seconds, with pay-as-you-go pricing. From data warehousing to deployment tools, directories to content delivery, over 200 AWS services are available and power hundreds of thousands of businesses in 190 countries around the world.

The AWS Cloud in Latin America has three Availability Zones within one geographic Region in São Paulo, Brazil, in addition to four Local Zones (Buenos Aires, Argentina; Lima, Peru; Querétaro, Mexico; and Santiago, Chile) and seven Edge Network locations (Bogota, Colombia; Buenos Aires, Argentina; Fortaleza, Brazil; Lima, Peru; Rio de Janeiro, Brazil; São Paulo, Brazil; and Santiago, Chile).

The new AWS Mexico (Central) Region, which will consist of three Availability Zones, is expected to launch by early 2025. As part of this investment, AWS is planning to invest more than $5 billion (approximately MXN $85 billion) in Mexico over the next 15 years.

Sustainability in Mexico

Amazon is deeply committed to investing in sustainable practices and driving innovation across its businesses to create a more environmentally responsible future for Mexico and the world. As a company at the forefront of sustainability efforts, we recognize the importance of minimizing our environmental impact while providing exceptional services to our customers.

As we expand our infrastructure and operations in Mexico, we are dedicated to building and operating our facilities in an eco-friendly and sustainable manner. Our state-of-the-art data centers are meticulously designed to deliver efficient and resilient services that meet the highest expectations of our customers, while simultaneously minimizing our environmental footprint and that of our clients. We use cutting-edge technologies and employ industry-leading practices to make sure that our operations are not only technologically advanced but also environmentally conscious.

Achieving emissions reductions

Amazon is steadfast in its commitment to reaching net-zero carbon emissions by 2040, as part of The Climate Pledge, aligning with the Paris Climate Agreement goals. Remarkably, we achieved our target of powering our data centers with 100 percent renewable energy by 2023, a full seven years ahead of schedule. According to FTI Consulting's analysis, the efficiency of public cloud computing in Mexico is projected to avert a staggering 158,000 metric tons of carbon emissions annually during the period of 2023 to 2038. This substantial reduction is equivalent to the carbon sequestered by nearly 2.6 million tree seedlings grown over a decade.

Moreover, Amazon's commitment to sustainability extends beyond its operations. For four consecutive years, Amazon has been the largest corporate purchaser of renewable energy globally, outpacing all other companies by a considerable margin, as reported by Bloomberg New Energy Finance (BNEF). In 2023, Amazon solidified its position as the world's leading corporate buyer of renewable energy.

Reducing water usage in AWS data centers

At AWS, we are committed to running our operations sustainably by minimizing both energy and water consumption in our data center operations. Our holistic approach starts with evaluating climate patterns, local water management, availability, and opportunities to use sustainable water sources. This guides the development of our water use strategy for each AWS Region, including our Mexico Region.

AWS has set an ambitious goal to become water positive by 2030. We are 41% of the way toward this target of lowering water use across our facilities by continually improving water efficiency through cloud technologies and investing in projects that return more water to communities than we consume. AWS' global water use efficiency metric of 0.19 liters of water per kilowatt-hour demonstrates our leadership in water efficiency among cloud providers.

We are actively using sustainable sources, such as recycled water and rainwater harvesting, wherever possible. Recycled water, suitable for applications like irrigation and industrial use, helps preserve valuable drinking water for communities. Additionally, AWS is investing in water replenishment projects to expand community water access, availability, and quality by restoring watersheds and bringing clean water, sanitation, and hygiene solutions. These efforts represent nearly 3.9 billion liters of water returned each year to the communities where we operate.

AWS will meet its water positive goals by employing four strategies:

- Water efficiency,
- Sustainable sources,
- Community water reuse, and
- Water replenishment.

In 2022, Amazon and Water.org announced a partnership to launch the Water.org Water & Climate Fund focused on climate-resilient water and sanitation solutions that will result in lasting access for 100 million people across Asia, Africa, and Latin America. A $10 million contribution from Amazon will directly empower 1 million people with water access by 2025, providing 3 billion liters of water per year in areas facing water scarcity.

AWS compliance programs

AWS has obtained certifications and independent third-party attestations for a variety of global and industry-specific workloads. The following are particularly relevant to Mexican organizations:

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 AWS SOC Reports:

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

An NDA is required to review the AWS SOC 1 and SOC 2 reports. The AWS SOC 3 report is a publicly available summary of the AWS SOC 2 report. The AWS SOC 3 report outlines how AWS meets the AICPA's Trust Security Principles in SOC 2 and includes the external auditor's opinion of the operation of controls. You can read the latest **AWS SOC 3 Report** on our website.

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the best practice guidance of ISO 27002. The basis of this certification is the development and implementation of a rigorous security program, including an information security management system that defines how AWS perpetually manages security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.

ISO 27017 provides guidance on the information security aspects of cloud computing; recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27001 and ISO 27002 standards. This code of practice provides additional information security control implementation guidance that is specific to cloud service providers. For more information, or to download the AWS ISO 27017 certification, see the ISO 27017 Compliance webpage.

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

ISO 27701 specifies requirements and guidelines to establish and continuously improve the privacy information management system (PIMS), including processing of personally identifiable information (PII). It is an extension of the ISO 27001 and ISO 27002 standards for information security management providing a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processors and controllers, not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.

ISO 22301 specifies requirements for an organization to implement, maintain, and improve a business continuity management system. Adherence to this standard makes sure that AWS has effective systems in place to prevent, prepare for, respond to, and recover from unexpected and disruptive events and helps customers achieve and maintain the highest-grade resiliency and security standards. For more information, or to download the AWS ISO 22301 certification, see the ISO 22301 Compliance webpage.

ISO 14001 is an internationally recognized standard for environmental management systems (EMS). It provides a framework for organizations to design and implement an EMS and improve environmental performance. Adherence to the standard helps organizations like AWS design their EMS to align with environmental compliance obligations, achieve environmental goals and

objectives, and enhance overall environmental performance over time. For more information, or to download the AWS ISO 22301 certification, see the ISO 14001 Compliance webpage.

AWS Artifact provides a central resource for AWS security and compliance reports. The artifacts available in AWS Artifact include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies that validate the implementation and operating effectiveness of AWS security controls.

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

Methods to prove compliance with the privacy laws

As mentioned at the beginning of this document, both LFPDPPP, which regulates the processing of personal data by the private sector, and LGPDPPSO, which regulates the processing of personal data by the public sector, state that a personal data Controller (as defined in section XXVIII of Article 3 of the LGPDPPSO and section XIV of Article 3 of the LFPDPPP) may use services, applications and infrastructure in the cloud as long as the cloud provider complies with certain requirements related to, among other things, the protection of privacy for personal data. This section demonstrates how AWS complies with these requirements.

The table in the next section is organized into the following columns:

- **Data controller obligations**: This column lists the obligations included in Article 63 of the LGPDPPSO and Article 52 of the LFPDPPP.
- **Methods to prove compliance**: This column lists AWS assets that customers can use to demonstrate compliance with their respective regulations based on INAI's Brief guide for obligated subjects for the contracting of cloud computing services that involve the processing of personal data.
- **Regulation**: This column indicates the regulations that the obligation and AWS solutions apply to.
- **AWS solutions**: This column explains the AWS resources that a data Controller can use to prove compliance with the law. Details on each best practice and associated AWS services that customers might use can be found in the linked resources.

#	Data controller obligations	Methods to prove compliance	Regulation		AWS solutions
			LFPDPPP	LGPDPPSO	
1.	Have and apply personal data protection policies in line with the applicable principles and duties established by this Law and other applicable regulations.	Request the Cloud Service Provider (CSP)'s Terms and Conditions governing the processing of content to verify that the Controller has complete control of the content that allows it to comply with the applicable principles and duties established by this Law and other applicable regulations.	X	X	AWS Customer Agreement AWS Data Processing Addendum AWS Service Terms As a customer, you control your content: • You determine where your customer content will be stored, including the type of storage and geographic region of that storage. • You choose the secured state of your customer content. AWS offers customers industry-leading encryption features to protect your content in transit and at rest and provides you with the option to manage your own encryption keys. • You manage access to your customer content, and access to AWS services and resources through users, groups, permissions, and credentials that you control.
2.	Make transparent the subcontracting that involves the information on which the service is provided.	Verify that CSPs are transparent about the subcontractors they use to process the information on which the service is provided.	X	X	AWS Sub-processors

#	Data controller obligations	Methods to prove compliance	Regulation		AWS solutions
			LFPDPPP	LGPDPPSO	
3.	Refrain from including conditions in the provision of the service that authorize or allow the CSP to assume ownership or property of the information on which it provides the service.	Verify that the CSP Terms and Conditions do not include conditions in the provision of the service that authorize or allow you to assume ownership or property of the information on which you provide the service.	X	X	AWS Customer Agreement AWS Data Processing Addendum AWS Service Terms
4.	Maintain confidentiality regarding the personal data on which the service is provided.	Verify that the CSP implements appropriate security standards in the services that Controllers use for personal data.	X	X	AWS Compliance Programs ISO 27001, ISO 27017, ISO 27018, ISO 27701, PCI DSS Level 1 and SOC 1, 2 and 3
5.	Inform the controller of any changes to its privacy policies or conditions of service provided so that, if necessary, the controller may inform data subjects of them.	Check the Terms and Conditions or other CSP mechanisms for the way in which the Controller may learn about changes to the Terms and Conditions.	X	X	AWS Customer Agreement AWS Data Processing Addendum AWS Service Terms AWS Privacy Notice

#	Data controller obligations	Methods to prove compliance	Regulation		AWS solutions
			LFPDPPP	LGPDPPSO	
6.	That the CSP allows the controller to limit the type of processing of personal data on which the service is provided.	Verify that the CSP Terms and Conditions allow the Controller to limit the type of processing of personal data on which the service is provided.	X	X	AWS Customer Agreement AWS Data Processing Addendum AWS Service Terms As a customer, you control your content: • You determine where your customer content will be stored, including the type of storage and geographic region of that storage. • You choose the secured state of your customer content. AWS offers customers industry-leading encryption features to protect your content in transit and at rest and provides you with the option to manage your own encryption keys. • You manage access to your customer content, and access to AWS services and resources through users, groups, permissions, and credentials that you control.
7.	Establish and maintain security measures for the protection of personal data on which the service is provided.	Verify that the CSP implements appropriate security standards in the services that Controllers use for personal data.	X	X	AWS Compliance Programs ISO 27001, ISO 27017, ISO 27018, ISO 27701, PCI DSS Level 1 and SOC 1, 2 and 3

#	Data controller obligations	Methods to prove compliance	Regulation		AWS solutions
			LFPDPPP	LGPDPPSO	
8.	That the CSP provides the Controller with functionalities that allow the deletion of personal data once the service provided to the Controller has concluded and the latter has been able to recover them.	Verify that the CSP allows Controllers to delete their content on demand. Controllers will have to delete the data once the service has ended since the CSP only allows the Controller to delete their information.	X	X	As a customer, you control your content: • You determine where your customer content will be stored, including the type of storage and geographic region of that storage. • You choose the secured state of your customer content. AWS offers customers industry-leading encryption features to protect your content in transit and at rest and provides you with the option to manage your own encryption keys. • You manage access to your customer content, and access to AWS services and resources through users, groups, permissions, and credentials that you control.
9.	That the CSP provides the Controller with functionalities to prevent access to personal data by persons who do not have access privileges, or, in the event that it is at the reasoned and motivated request of a competent authority, inform the Controller of that fact.	Verify that the CSP provides the Controller with tools to control access to its content in the cloud, including personal data.	X	X	AWS customers can prevent access to their data using AWS Identity & Access Management (IAM) and AWS security, identity, and compliance services, including Amazon Cognito, AWS Organizations, Amazon GuardDuty, AWS Security hub, and others.

Steps to use the public cloud procurement framework

On April 18th, 2024, the Mexican federal government established the Contrato Marco for the public cloud procurement framework (hereafter referred to as the *Contrato Marco* or *procurement framework*). This new procurement framework aims to streamline the public cloud procurement process for government agencies (Dependencia o Entidad de la Administración Pública Federal).

As an initial step, AWS has joined the procurement framework along with a select group of partner vendors. Under the procurement framework, government agencies must conduct expedited tender processes using the standardized terms and conditions of the procurement framework. Agencies can add their specific requirements and request quotes from the qualified vendors participating in the procurement framework.

Regarding vendor compliance, organizations must submit required documentation at two stages: first, when joining the procurement framework, and then again with updated versions for each individual agency tender process. The mandatory documentation includes administrative information about the vendor (for example, certificates of incorporation, bylaws, and tax ID), affidavits confirming compliance with the procurement framework's terms and conditions, in addition to various security and quality certifications such as ISO 9001, 27001, 27017, 27018, 22301, 14001, PCI DSS, and FIPS 140-2 Level 2. Additionally, partner vendors must submit updated letters of support from AWS for every tender.

The tender process under the procurement framework follows these steps:

1. The agency develops a requirements document using the procurement framework's provided template.
2. The agency submits the requirements document and creates the tender entry on the CompraNET platform, specifying the dates and service quantities requested.
3. All vendors participating in the Contrato Marco receive an invitation to submit proposals.
4. The agency opens a period to receive and respond to questions and clarification requests on CompraNET.
5. The agency provides responses to all questions and requests received.
6. Vendors can then submit their proposals through CompraNET.
7. The agency can either award the contract or restart the process if the submissions are not satisfactory.

The entire tender process under the procurement framework is designed to take 1–2 months, which is significantly faster than the 2–6 months (or longer) typical of traditional procurement procedures.

Additional resources

The following are additional resources to help Mexican organizations think about security, compliance, and designing a secure and resilient AWS environment.

- AWS supports 143 security standards and compliance certifications, including ISO 27001, ISO 27017, ISO 27018, ISO 27701, PCI DSS Level 1, and SOC 1, 2, and 3. AWS implements and maintains technical and organizational security measures applicable to AWS cloud infrastructure services under globally recognized security assurance frameworks and certifications. Additionally, AWS provides on-demand access to security and compliance reports (through the automated compliance reporting portal available in the AWS Management Console) from the AWS environment through AWS Artifact. Customers can download reports and details about more than 2,600 security controls.
- Proprietary virtualization system: The AWS Nitro System is the foundation of the AWS sovereign cloud stack. It provides a strong physical and logical security boundary to enforce access restrictions so that nobody, including AWS employees, can access customer data running in Amazon EC2. The security design of the Nitro System has been independently validated by the NCC Group in a public report.
- AWS Control Tower: offers guardrails to provide more control over the physical location of where customer data is stored and processed (over 245 controls are available under the digital sovereignty category grouping), a concept known as data residency (data is not stored or processed outside a specific AWS Region or Regions).
- Encryption: features and controls to encrypt data, whether in transit, at rest, or in memory. AWS services support encryption—with most also supporting encryption with customer managed keys that are inaccessible to AWS—with encryption keys managed inside or outside the AWS Cloud.
- AWS Compliance Quick Reference Guide: AWS has many compliance-enabling features that you can use for your regulated workloads in the AWS Cloud. These features help you to achieve a higher level of security at scale. Cloud-based compliance offers a lower cost of entry, more straightforward operations, and improved agility by providing more oversight, security control, and central automation.
- AWS Well-Architected Framework: The AWS Well-Architected Framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. The framework consists of six pillars: Operational Excellence, Security, Reliability, Performance Efficiency, Cost Optimization, and Sustainability. 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.
- NIST Cybersecurity Framework (CSF): The AWS whitepaper NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud demonstrates how public and commercial sector organizations can assess the AWS environment against the NIST CSF and improve the security measures they implement and operate (that is, security in the cloud). The whitepaper also provides a third-party auditor letter attesting to the AWS cloud offering's conformance to

NIST CSF risk management practices (that is, security of the cloud). Defense and security organizations can use NIST CSF and AWS resources to elevate their risk management practices.

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

Getting started

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

For public organizations in Mexico, next steps typically include the following:

- Contact your AWS representative to discuss how the AWS Partner Network, AWS Solution Architects, Professional Services teams, and Training instructors can assist with your cloud adoption journey. If you do not have an AWS representative, contact us.
- Obtain and review a copy of the latest AWS SOC 2 reports and ISO 27001 certification from the AWS Artifact portal (accessible through 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 considering your due diligence and risk assessment, using the tools and resources referenced throughout this guide and in the Additional Resources section.

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

Contributors

Contributors to this document include:

- Arturo Cabanas, Principal Security Assurance and Compliance, AWS
- Michael Davie, Specialist Security Assurance and Compliance, AWS
- Carlos Borella, Specialist Security Assurance and Compliance, AWS

Document revisions

Date	Description
December 2024	First publication