



Regulatory Overview

Financial Services — Argentina

AWS is committed to offering financial institutions in Argentina a strong compliance framework and advanced tools and security measures which they can use to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements.

This document provides AWS financial institution customers with information about the legal and regulatory requirements in Argentina which may apply to their use of AWS services.

Financial institutions in Argentina are **permitted** to use cloud services, provided that they comply with applicable legal and regulatory requirements, such as those described below.

Who is the financial regulator in Argentina?

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

The Comisión Nacional de Valores, or “CNV” (National Securities Exchange Commission), regulates the Argentinean capital markets, including stock exchanges, agents, brokers, listed corporations, and investment funds.

The Superintendencia de Seguros de la Nación, or “SSN” (National Superintendence of Insurance), regulates the insurance market and insurance companies.

What regulations apply to financial institutions in Argentina using AWS?

Financial institutions in Argentina may be subject to a number of different legal and regulatory requirements when they use cloud services. Relevant regulations include:

- BCRA [Communication “A” 6,354 of November 3, 2017](#), as amended by [Communication “A” 6,375 of November 17, 2017](#), establishes general outsourcing guidelines that banks and financial institutions regulated by the BCRA must follow when procuring IT services, including cloud services. In addition, the BCRA issued a [public interpretation](#) of certain matters related to [Communication “A” 6,354](#), clarifying BCRA’s position with respect to cloud services.

Customers that have questions about the applicable regulations and guidelines, and how these may apply to their use of AWS services, can reach out to their account representative or [contact us](#).

Regulations are changing rapidly in this space, and AWS is working to help customers proactively respond to new rules and guidelines. AWS encourages its financial institutions customers to obtain appropriate advice on their compliance with all regulatory and legal requirements that are relevant to their business, and local regulations, guidelines and laws.



Key considerations for financial institutions in Argentina using AWS

AWS is committed to offering customers a strong compliance framework and advanced tools and security measures which customers can use, to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements.

Financial institutions who are using or planning to use AWS services can take the following steps to better understand their compliance needs:

- 1 Consider the purpose of the workload(s) under consideration and the relevant categories of data in order to anticipate which legal and regulatory requirements may apply.
- 2 Assess the materiality or criticality of the relevant workload(s) in light of local requirements. For example, [Communication "A" 6,375](#) contains materiality assessment considerations for financial institutions.
- 3 Review the AWS [Shared Responsibility Model](#) and map AWS responsibilities and customer responsibilities according to each AWS service that will be used. Customers can also use [AWS Artifact](#) to access AWS' audit reports and conduct their assessment of the control responsibilities.
- 4 Customers that have further questions about how AWS services can enable their security and compliance needs, or that would like more information, can contact their account representative or contact us.

If you have questions about using AWS services or need more information, please [contact us](#).

Key data privacy and protection considerations for financial institutions in Argentina using AWS

Financial institutions in Argentina using AWS services should also consider applicable privacy requirements, including Argentina's [Personal Data Protection Law No. 25,326](#) ("PDPL") as supplemented by [Regulatory Decree No. 1558/2001](#) and supplementary regulations.

The Argentine Data Protection Authority issued [Resolution No. 47/2018](#) under the PDPL, describing a catalogue of recommended security measures that financial institutions should consider depending on the activities they conduct or the nature of the personal data that they process.

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.



Additional AWS Resources

- [AWS Compliance Quick Reference Guide](#)
- [Using AWS in the Context of Common Privacy and Data Protection Considerations](#)
- [Argentina Data Privacy](#)

Additional AWS Resources - Spanish

- [Guía de Referencia Rápida sobre Seguridad y Conformidad de AWS](#)
- [Privacidad de los datos en Argentina](#)

AWS Compliance Programs



CSA



GDPR



ISO 9001



ISO 27001



ISO 27017



ISO 27018



PCI DSS Level 1



SOC

This document is provided for informational purposes only. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.