Regulatory Overview

Financial Services — Canada

AWS is committed to offering financial institutions in Canada 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 Canada which may apply to their use of AWS services.

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

Who are the financial regulators in Canada?

The Office of the Superintendent of Financial Institutions, or "OSFI" is the federal regulator for all banks in Canada, and federally incorporated or registered trust and loan companies, insurance companies, cooperative credit associations, fraternal benefit societies and private pension plans. OSFI is responsible for supervising federally regulated financial institutions and pension plans to determine whether they are in sound financial condition and compliant with applicable requirements. It also issues regulations and guidance that may affect how financial services customers use AWS.

The Bank of Canada, Canada's central bank, has direct oversight over clearing and settlement systems, that is, financial market infrastructures (FMIs). The Bank of Canada has the ability to designate certain financial market infrastructures as "prominent payment systems" or "systemically important FMIs" and requires financial market infrastructures to comply with risk management standards.

Each Canadian province and territory has its own regulator to enforce securities regulations. The Canadian Securities Administrators is an umbrella organization comprised of the securities regulators from each province and territory with an objective of improving, coordinating, and harmonizing securities regulation.

What regulations apply to financial institutions in Canada using AWS?

Financial institutions in Canada may be subject to a number of different legal and regulatory considerations when they use cloud services. Relevant regulations and guidelines for federally regulated financial institutions ("FRFIs") include:

- OSFI **Guideline No. B-10** sets out OSFI's expectations for managing risks associated with third-party arrangements. The Guideline applies to all third-party arrangements including cloud services, but OSFI's expectations are scaled based on the assessed level of risk and the criticality of the arrangement to the financial institution's operations. B-10 includes specific expectations for the management of technology and cyber risk in third-party arrangements, as well as expectations specific to cloud adoption.
- OSFI **Guideline No. B-13** outlines OSFI's expectations for the sound management of technology and cyber risk. While there are no requirements specific to cloud services, the outcomes, principles, and expectations apply to all aspects of technology and cyber risk management, including cloud computing.
- OSFI **Guideline No. E-21** sets out OSFI's expectations for regulated entities' management of operational risk, defined as "the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events." While not specific to the use of cloud, the expectations in this guideline apply to all aspects of a regulated entity's operations, including those enabled by cloud services.

- OSFI's advisory on **Technology and Cyber Security Incident Reporting** governs how federally regulated financial institutions should disclose and report technology and cyber security incidents to OSFI.
- OSFI also released an updated **Cyber Security Self-Assessment** that helps FRFIs gauge and improve their current state of readiness with respect to emerging cyber threats. The Cyber Security Self-Assessment examines a FRFI's capability to respond to a cyber incident in areas ranging from organization and resources, to how it manages threats, risks and incidents, and allows FRFIs to rate each element on a scale from non-existent to continuous improvement.
- The Bank of Canada has published **risk-management standards for designated FMIs** based on the "Principles for FMIs" established by the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). In addition to these general standards for risk management, the Bank of Canada has published specific guidelines on **Expectations for Cyber Resilience of Financial Market Infrastructures** and **Cyber and Information Technology Incident Reporting**.

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 institution 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 Canada 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 level of risk and criticality of the relevant workload(s) with respect to the financial institution's operations. **Guideline No. B-10** outlines considerations for assessing the risk and criticality of third-party arrangements.
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's 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.

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

Financial institutions in Canada using AWS should also consider applicable privacy requirements, including Canada's **Personal Information Protection and Electronic Documents Act "PIPEDA"**, a Canadian federal law regulating the collection, use, and disclosure of personal information in the course of commercial activities in all Canadian provinces.

Certain Canadian provinces have adopted privacy legislation substantially similar to PIPEDA. Customers should consult their own legal advisors to understand the privacy laws to which they are subject. An updated list of privacy regulations can be found in the Data Privacy Center.

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

- Canadian Centre for Cyber Security (CCCS) Assessment
- AWS User Guide to Canada's Controlled Goods Program (CGP)
- AWS Compliance Quick Reference Guide
- Using AWS in the Context of Common Privacy and Data Protection Considerations

AWS Compliance Programs

CSA

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.