Canada's Evolving Regulatory Framework

for Cloud-Based Financial Services

September 2020

Wilson Center
CANADA INSTITUTE

aws institute

About the AWS Institute

This paper was co-produced by the AWS Institute and the Canada Institute. The AWS Institute convenes and engages global leaders who share an interest in solving public sector challenges using technology. For more information about the AWS Institute, please visit: https://aws.amazon.com/institute/

If you would like to offer feedback on this paper, please email aws-institute@amazon.com

About the Canada Institute

The Wilson Center's Canada Institute is the only public policy forum in the world dedicated to the full spectrum of Canada-U.S. issues. Based in Washington, D.C., the Canada Institute is a global leader for policymakers, academics, and business leaders to engage in non-partisan, informed dialogue about the current and future state of the relationship.

Table of contents

Executive summary

Digital transformation in the global banking industry requires Canadian financial services regulators to consider how to update rules and procedures created for traditional banking and financial services to reflect the new realities of financial services—increasingly conducted online and in the cloud. The challenge that governments and business face is how to uphold their longstanding objectives of customer security and financial stability while also helping to create an environment that enables innovation.

The stakes are high. Canada's financial system has long been a global model of stability and security, consistently ranking among the top two or three in the world for soundness of banks At the same time, Canadian firms are unable to take advantage of the same opportunities as competitors in other parts of the world—due in part to regulatory gaps and uncertainties. Cloud-based storage and computing pose a particular challenge for regulators because there is a continuing bias towards on-premises infrastructure. Even though, there is ample evidence that hyperscale cloud service providers like AWS enable organizations to strengthen their own compliance and certification programs and automate manual security tasks so they can shift their focus to scaling and innovating.

To provide Canadian customers with the financial services they demand and position Canadian firms for global competitiveness, industry representatives recommend that new rules around the use of technology in the financial services sector be clear and transparent. They also recommend that government and industry work together to eliminate unnecessary duplication between jurisdictions and that regulators seek to understand better the security benefits of cloud storage facilities as compared to on-premises infrastructure.

Consumers today expect financial services to be simple: they purchase goods or services on

Introduction

a mobile phone while watching television or waiting to board a plane and they want the same convenience when managing their finances.[1] Not that long ago, such transactions would have been impossible without a trip to the bank. Today, financial institutions demonstrate how much the landscape has changed. A case in point is the UK's Starling Bank. It has no physical branches, but it is consistently voted one of Britain's top banks for customer service. Fintech companies have emerged in every financial services vertical for money transfer, e-credit card, and lending solutions, among other services.[2] Much of the convenience and availability of new services can be attributed to the rise of cloud technology.

But, customer convenience is only part of the story. Cloud-based technologies are enabling financial services institutions (FSIs) to provide innovative products while also enhancing their security, data storage capacity, and computing power. McKinsey & Co. forecasts that between 40 and 90 percent of bank activities globally could be done in the cloud by the late 2020s.

At the same time, new technologies raise questions about how to ensure that new ways of doing things are compatible with the bedrock priorities of consumer protection and the stability of the national and global financial systems. As cloud becomes an integral part of financial service delivery, regulators in Canada and around the world are seeking to understand how to fully leverage the security and innovation that cloud provides within a framework of regulations and enforcement procedures intended for brick-and-mortar FSIs.

This report examines how Canada's financial services sector is taking advantage of cloud computing to compete in a rapidly changing marketplace, and it describes how the evolving regulatory framework will affect the sector's ability to compete globally. The report draws from insights provided by finance industry leaders who shared their perspective with the authors at a roundtable hosted by the Canada Institute and the AWS Institute in Toronto, Ontario on July 18, 2019.[3] The recommendations presented in this report are drawn from that conversation.

Digital transactions now dominate the financial services industry. Canadian consumers have

1 A 2019 poll done for the Canadian Bankers Association showed that 32 per cent of Canadian financial transactions take place on a mobile device. That percentage is expected to jump to 41 per cent by 2024.
2 See, for example, TransferWise, NuBank and Robinhood.
3 On July 18, 2019, the Wilson Center's Canada Institute and the AWS Institute hosted a stakeholder roundtable in Toronto, Ontario entitled "Moving Canada's Financial Sector Forward: Building Smart Policies for Smart Technologies." The invitation-only event brought together policy, industry, and academic experts to discuss financial sector adoption of cloud-based processes. The meeting observed Chatham House rules and the report paraphrases participant comments, except when cited with the permission of the speaker.

The opportunity: Canada's financial services industry in transition

signalled a growing comfort with digital technologies in their financial services transactions. According to the most recent survey data from the Canadian Bankers Association, most Canadians (91 percent) believe that banking has become a lot more convenient because of new technologies and more than 85 percent of Canadians feel confident about modern banking technologies and trust their bank to offer secure digital services.

Despite consumer confidence and demand, Canadian financial institutions are moving at a slower pace than their global competitors. Canadian firms have begun migrating their operations to the cloud but have yet to seize the opportunities in ways that bankers in countries such as Australia, the UK, and Singapore have done. Jon Spinks, chief executive officer of Sourced, a Toronto-based consulting firm that assists companies to move operations to hyper-scale cloud providers, confirms that Canadian companies are moving incrementally; nevertheless, he anticipates "a huge amount" of future opportunity.[4]

FSIs that have already moved their data storage to the cloud have seen growth in their

4 Authors' interview, Toronto, June 20, 2019.

The Cloud advantage: Performance and security

ability to offer new services, as well as enhanced security. Some of world's largest financial entities are embracing the cloud, even those considered traditionally conservative. The Bank of England, for example, has put cloud adoption at the forefront of its banking modernization strategy.

In the United States, the Financial Industry Regulatory Authority (FINRA), which regulates brokerage firms, has migrated 90 percent of its data volume to cloud. In order to protect individual investors and the stability of the financial system, FINRA must capture and analyze some 37 billion records per day. With the robust security and rapid scalability of the cloud, FINRA can better fulfill its mission, especially during period of market volatility when daily record counts can double or triple.

In Australia—a country with a market and regulatory system comparable to Canada's—the Australia Financial Group shifted its entire IT operation to cloud. Before the shift, the Group spent more than 80 percent of its IT budget on operational costs. Migrating operations to cloud reduced costs and allowed the company to change its tech spending so that 60 percent is now devoted to innovation.

Closer to home, the National Bank of Canada uses cloud to manage the analytics for its exchange-traded securities. The bank's General Equities Derivatives Group bases its trading decisions on current and historical financial market data. Previously, the bank's on-premises hardware and databases were only able to manage about 10 percent of the questions that analysts wanted to answer. Today, using cloud-based technologies, analyses that used to take days only take minutes.

Chris Enright, President and Managing Director of Canada's Aligned Capital Partners, provides another example of how migration to a cloud platform improved his company's efficiency. "In the past, when we brought a new financial advisor onboard with an established book of business from another institution, the paperwork required to make this transition involved several thousand pages of forms that took an advisor approximately two months to complete. With a digital platform using cloud technology, this process can now be done in 72 hours."[5]

A key advantage of the cloud is enhanced security. For example, vulnerability to malicious

5 Chris Enright presentation at Wilson Center/AWS Roundtable, Moving Canada's Financial Sector Forward: Building Smart Policies for Smart Technologies, Toronto, Ontario, July 18, 2019.

attacks is significantly reduced because customers can elect to store their data in multiple, physically separated, and isolated sites around the world. The data is subject to continuous testing to provide stability within a changing threat landscape. Reporting from the Depository Trust & Clearing Corporation (DTCC) notes that cloud vendors provide more capability, security of service, and resilience than most on-premises data centers.

For larger FSIs, the security and compliance benefits of cloud-based service providers helps to simplify, protect, and transform complex, legacy infrastructure to achieve equal or better levels of assurance with less effort.[6] This is a huge advantage for small- and medium-sized enterprises, since the cloud enables them to operate IT environments with levels of security, resilience, and state-of-the-art technology traditionally available only to the largest companies.

Looking through a regulatory lens, the most important benefit of the cloud is the potential to safeguard the stability of national and global financial systems. Cloud practitioners achieve this by reducing vulnerability to cyber attacks through fine-grained access controls, and detailed logging, monitoring, and analytics capabilities.

A 2018 FINRA blog post provides a real-world illustration:

> To do our job of protecting investors and ensuring market integrity, it's important that we are on top of each day's activity, applying our automated surveillance patterns to help our analysts look for potentially suspicious activity—instead of running to catch up. In our role as a regulator, we must often access data from weeks or months ago. When you have tens of billions of records to process every day, and you are storing that data for months or years at a time to analyze historical trading patterns, that means you have a lot of data—28 petabytes of data, to be exact. That's enough data to play 40,000 years of music—without any repeats or interruption.

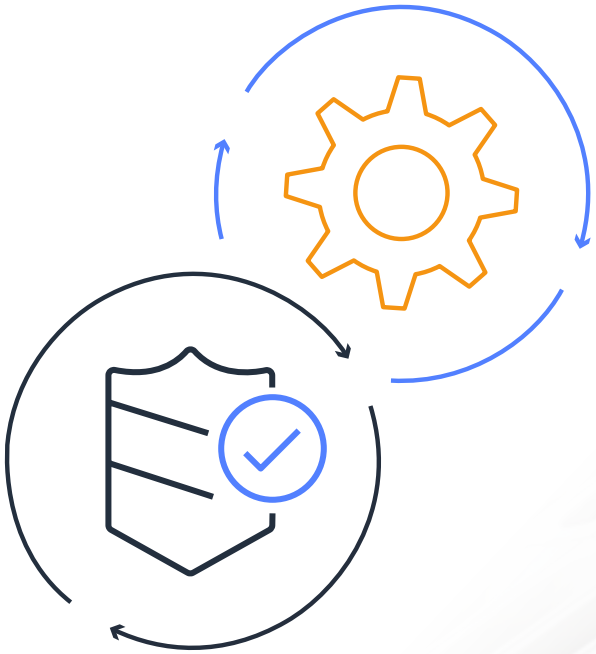
The adoption of new technologies demands regulatory upgrades that support new ways

6 See AWS White Paper, Cybersecurity in the Financial Services Sector (July 2019).

Regulatory modernization

of doing business while protecting consumers and the financial system as a whole. DTCC deems regulatory compliance risk as the "last hurdle" to widespread cloud adoption by financial services. The challenge of regulatory modernization is complex. What rules need to be changed? Where are new rules needed? How will new rules be monitored to ensure they are working as they are supposed to?

This is the transitional phase that Canada is working through today. While there are models emerging from other countries and international organizations, there are no easy answers or quick fixes. In the meantime, the clearest recommendation from industry is that regulators need to solicit input from firms and customers throughout the process while working with peers inside and outside the country to create regulatory harmonization and minimize duplication.



Canada's regulatory framework

In Canada, financial services are regulated at both the federal and provincial/territorial levels. The federal government is responsible for supervising all banks, federally incorporated insurance companies, trust and loan companies, cooperative credit associations, and federal pension plans. The Office of the Superintendent of Financial Institutions (OSFI), an independent federal agency, oversees more than 400 financial institutions and 1,200 pension plans to ensure that these federally regulated entities (FREs) are in sound financial condition and meeting their requirements.

Provincial governments are responsible for supervising securities dealers, mutual fund and investment advisors, credit unions, and provincially incorporated trust, loan, and insurance companies. The securities commissions in Ontario, British Columbia, Quebec, and Alberta are the most significant regulators of investment dealers and brokers. They are loosely confederated under the Canadian Securities Administrators (CSA).[7]

OSFI's approach to regulation

OSFI's main functions are regulation and supervision. As a regulator, OSFI develops and interprets rules and provides regulatory approvals for the transactions within its scope. As a supervisor, OSFI is concerned with the soundness of the financial system. It analyzes financial and economic trends to identify issues that could adversely affect FREs.

Although it monitors both larger trends and the activity of individual institutions, OSFI does not take a hands-on role in the operations of FREs, leaving responsibility for actions and decisions in the hands of company managers and their boards. It also acknowledges the importance of competitiveness. As the OFSI website notes:

> Financial institutions must be allowed to take reasonable risks and compete effectively both at home and abroad, while at the same time safeguard the interests of depositors, policyholders, beneficiaries, and pension plan members. OSFI's goal is to balance competitiveness with financial stability and international standards with Canadian market realities.

7 Although the CSA is not a direct governing body of securities firms the way that OSFI is for deposit-taking institutions, it issues guidelines that may be adopted by provincial securities regulators.

Managing risk

Financial risk includes material risks such as credit risk (the likelihood that borrowers will pay back their loans) and liquidity risk (the ability of a bank to meet its obligations to its depositors). Financial institutions must also manage operational risks. These include losses due to errors, breaches or other damages caused by people; as well as losses due to internal processes, systems or external events. Some of the perceived risks related to digital transformation are in the operational risk category. These include cybersecurity, outsourcing, concentration, and data residency.[8]

Cybersecurity

Cybersecurity tops the list of preoccupations for regulators. FSIs, their customers, and the national or even global financial system can face catastrophic consequences if malicious actors gain access to critical functions or processes. In the Canadian context, such incidents trigger mandatory reporting obligations to regulators including OSFI[9] and provincial securities regulators. Provinces and territories also require FSIs to maintain compliance systems that defend against cyber threats. Any organization that is compromised must immediately report breaches to the Privacy Commissioner of Canada.[10]

While recognizing the seriousness of cyber attacks, the industry recommends against a one-size-fits-all approach to security. Instead, security protocols should be aligned with levels of risk, scaling upwards or downwards commensurate with the severity level of the potential harm. Financial services companies also recommend that there be variable levels of security assigned to protect client information, depending on what type of data the companies possess and its sensitivity.

Outsourcing

OSFI views cloud migration as a type of outsourcing and therefore applies the guidelines found in its B-10 Memorandum on Outsourcing of Business Activities, Functions, and Processes. In general terms, OSFI advises that FSIs are ultimately accountable for activities performed by third parties and their compliance with OSFI rules.[11]

8 While beyond the scope of this paper, it is important to note that this section deals with perceived risks. In practice, public and private sector organizations are listing antiquated technology, manual/time intensive processes, and skills gaps among their most pressing concerns. See The Risk of the Digital Status Quo: How Governments Can Enable Digital Transformation (2019, Public Policy Forum).
9 OSFI has created Cyber Security Self-Assessment Guidance to help entities understand and manage reportable incidents.
10 Privacy breach notifications are covered by Canada's breach notification regulations were introduced pursuant to the 2000 Personal Information and Electronic Documents Act.
11 Similar guidance is provided to Canadian securities firms by the CSA.

OSFI guidance on outsourcing takes the form of specific principles and expectations but these are not mandatory requirements. FSIs are asked to interpret the expectations and implement policies in ways consistent with their organization's own risk management programs. While this approach provides the flexibility that FSIs usually prefer, some industry representatives are experiencing a measure of uncertainty derived from having to apply new and relatively untested rules and procedures.

The industry recommends that guidance from OSFI be more clearly defined, especially for significant actions such as cloud migration. This will create greater certainty, which, in turn, allows businesses to plan and invest appropriately.

Concentration

The use of new technologies from third-party providers raises questions about the risk of concentration, i.e. the vulnerabilities that arise from over reliance on too few service providers.

The counter-argument, however, is that concentration risk is significantly reduced when using cloud systems compared to on-premises systems where all vulnerabilities are concentrated in a single or small number of data centers. Cloud service providers distribute encrypted applications and data throughout millions of servers in dozens of data centers. A 2019 article in CPA Practice Advisor, the magazine of Canada's professional accounting industry, notes that data stored in the cloud is far less vulnerable to physical harm since"reputable cloud service providers have geographically dispersed, high-tech, highly secure data centers to ensure that if your data is compromised in one place, it is secure in another."

The use of physically isolated Availability Zones – clusters of data centers connected by low latency, high throughput, and highly redundant networking – offer FSIs a more effective way to design and operate applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter or multi-datacenter infrastructures.

In testimony to the House of Commons, the AWS Director of the Office of the Chief Information Security Officer Mark Ryland explained that the continuous evolution of threats means that cloud service providers must be constantly evolving their technologies to stay ahead. This is one area where a cloud provider's size and access to resources make a difference. Ryland said, "Economies of scale mean that cloud providers can develop and launch new services and security offerings faster than ever before. This provides organizations such as financial institutions with modern capabilities to stay ahead of malicious threat actors."

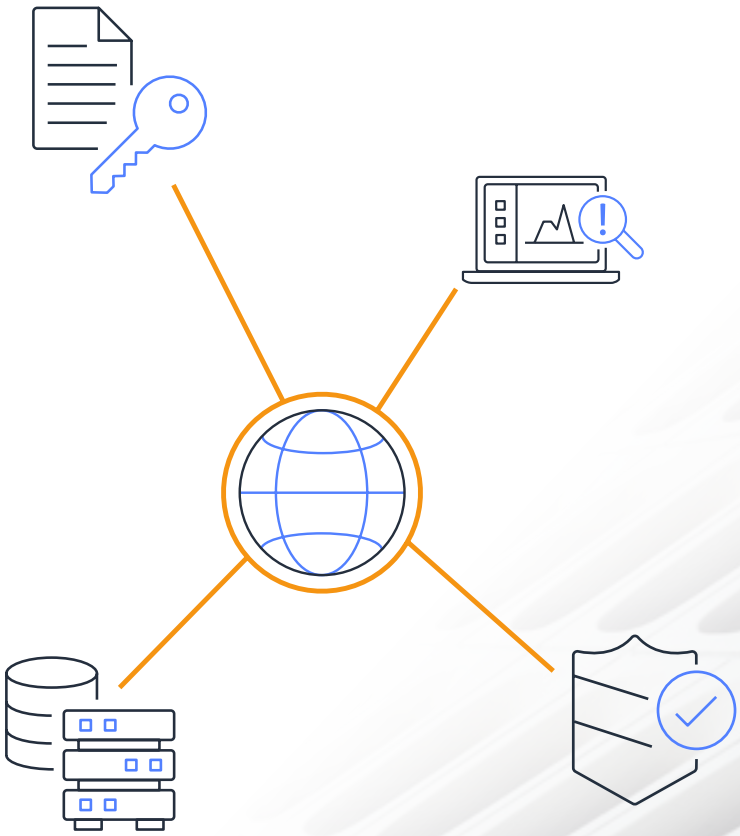
Data residency

The geographic location of data storage sites is a central preoccupation in the formation of digital policy. Because of the United States's significant influence on Canada's economic and cultural affairs, Canadians are particularly sensitive to issues of data privacy and

sovereignty. Many hold the view that Canadians' data is safer when kept within national borders. However, as the prior discussion on cybersecurity emphasizes, geography is not the same as security. Data localization does not enable organizations to full diversify risks and could reduce their ability to design resilient services built on multi-region/multi-zone architectures. As Mark Ryland said, "Keeping data locally does not mean it is more secure, nor do users of cloud services get the full benefits of stronger security and flexible infrastructure if data must be maintained locally."

At present, Canada's financial regulators continue to require that certain types of records listed in the Bank Act, the Insurance Companies Act, the Trust and Loan Companies Act, and the Cooperative Credit Association Act reside in Canada. The new US-Mexico-Canada (USMCA) trade agreement may help to reduce data localization restrictions among the three countries.

Business stakeholders advise that data localization rules hamper innovation and impede cybersecurity response. One executive explained that data residency rules make it difficult for his company to aggregate data across borders to perform the kind of analytics and artificial intelligence (AI) functions that the industry demands. She or he also noted that data residency also make it harder to respond to transnational cybersecurity risks. The executive recommends that better co-operation and harmonization among regulatory agencies should be sufficient to address most concerns about access to data.



Is Canada keeping up with global peers?

Canadian industry executives are concerned that regulatory guidance is much further ahead in places like the UK and Europe, which diminishes Canadian competitiveness vis-à-vis peer markets.

The Australia Prudential Regulation Authority and the Monetary Authority of Singapore have both released recent guidelines that situate the competitive benefits of cloud technology within the context of a secure regulatory framework. Similar guidance is expected from Britain's Prudential Regulatory Authority. One of main champions of regulatory modernization in the UK has been Canadian Mark Carney in his capacity as governor of the Bank of England. In a 2019 speech, Carney forcefully argues for the importance of innovation for the success of the financial services industry.
The City of London has maintained its pre-eminence by innovating. This was as true in the First Industrial Revolution when finance oiled the pistons of the steam engines as it is today at the dawn of the Fourth Industrial Revolution, with the advent of cloud computing and the robosapien fund manager. Today the key competitive advantage in financial services is how firms—and supervisors—collect, store, and analyse the explosion of data. Just as the steam engine transformed manufacturing, AI, machine learning (ML), and cloud- based technologies are transforming services.

Industry representatives note that Canadians are seeing financial services and products that are available in other countries and are frustrated when they can't access these at home. They observe that the regulatory agencies in the world that are the most forward thinking are those that ask whether their rules are inhibiting technological innovation that would enable companies to develop better products and services for consumers. The industry recommends that when regulators consider procedures intended for customer protection that they also consider customer service—this approach will help to optimize the balance of security and innovation.

Guidance from international organizations

International organizations such as the G7 and G10 are important sources of information and best practices for financial services regulators. Not only do international organizations (IOs) help to inform national policy and facilitate harmonization across jurisdictions, they provide a confidential space where officials can discuss problems and concerns without signaling a specific vulnerability to malicious actors.12 Now, more than ever, governments are seeking IO input to guide national regulators through the complex process of digital transformation. While this work moves slowly, it should eventually yield substantive results, underpinned by broad international consensus.

Regulatory discontinuity between countries is not the only challenge for Canadian FSIs. A 2017 Competition Bureau report identifies inconsistencies between federal and provincial rules as both a barrier to financial services innovation and a drag on Canadian competitiveness overall. Industry representatives recommend that focusing on rules harmonization will help facilitate competiveness, encourage innovation, bolster security, and strengthen rules enforceability.

12 One of the most influential sources of global policy guidance is the G7 Cyber Expert Group. Made up of the finance ministries, central banks and supervisory authorities of the world's leading economies, this group provides updated guidance documents on key cybersecurity concerns. Recognizing that common language is key to common understanding, the G-20, has published a Cyber Lexicon to provide financial sector authority with a common understanding of relevant terminology. Some important work is also taking place at the sectoral level. See, for example, the Basel Committee on Banking Supervision, and the International Organization of Securities Commissions. The International Association of Insurance Supervisors is expected to offer its own guidance shortly.

Where does this leave Canada?

The regulatory environment in Canada provides a strong risk management framework that meets current needs while allowing room for future development. However, since many of the emerging guidelines for digital transformation have not been tested, institutions do not have the certainty they would prefer for future planning. These gaps, if not addressed, will become more evident as the government of Canada continues to advance its digital innovation agenda.

Summary of recommendations

1. Align escalating security protocols with the proportionate level of risk.
2. Assign different levels of security to protect different types of customer information, according to degree of sensitivity.
3. Work to integrate customer-service considerations into security planning.
4. Avoid or eliminate data localization rules since they provide little security benefit and are a drag on innovation and competitiveness.
5. Provide businesses with more certainty in the interpretation of rules and procedures.
6. Once rules are clearly defined, develop mechanisms to test and refine their application.
7. Wherever possible, harmonize rules and procedures within and across jurisdictions. International organizations can facilitate this process but they are not equipped to lead. Underpinning its need to deliver better digital services with agility and speed while minimizing cost, the Government of Canada announced its Cloud Adoption Strategy in 2016. The program intended to establish a cloud-first approach for the delivery of federal IT services. By late 2019, this strategy had advanced only to a limited extent.