Deloitte.

Strengthening resilience

2019 Canadian regulatory outlook for financial institutions

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Contents

Foreword

Introduction

Nearly ten years after the financial crisis, the long shadow it has cast has started to fade. With the exception of one final component of Basel III, most post-crisis prudential policies have now been decided, and banks in particular are now much better capitalized and more liquid than before the crisis. Amid varied approaches and timetables to national implementation of agreed prudential reforms, attention is now more acutely focused on culture and governance, the challenges of new technology, and emerging economic, market, and operational risks. Firms need to be prepared to respond to this shifting focus and the new demands that it will place on them.

Lifting of accommodative monetary policy

Globally, monetary easing and low interest rates are slowly giving way to interest rate normalization, although rates are expected to settle at levels significantly below historical norms. The US has led the way with a series of rate rises and the Federal Reserve has begun to shrink its balance sheet. The Bank of England has tentatively begun to raise rates, and the European Central Bank is bringing an end to the expansion of its balance sheet. In Australia, interest rates remain on hold but are expected to begin rising. Japan is the major exception to this trend, with rates expected to remain low in the near future. Given the number of headwinds to the global economy (e.g., high levels of debt, elevated levels of geopolitical risk, and trade protectionism), the pace of any interest rate rises is likely to be slow.

Higher interest rates may be beneficial in net terms to certain firms: banks may enjoy higher net interest margins and insurers could benefit from rising asset yields. However, interest rate normalization may also lead to falls in some asset values and rising credit defaults as well as revealing structural weaknesses in both the global economy and individual firms. It is unclear what the overall effect of these opposing factors will be, especially at the level of individual firms and sectors.

An uncertain economic environment

Meanwhile, a period of accommodative monetary policy has contributed to a build-up of debt, with global debt levels now at $247tn[1], significantly higher than their pre-crisis peak. In many commentators' eyes, this represents a key systemic vulnerability[2]. Low rates also contributed to a sustained search for yield that may have led many lenders and investors to move down the credit quality curve. Further, comparatively higher capital requirements for banks have paved the way for a rise in non-bank lending, which means that exposure to credit markets now extends to a much wider variety of firms. Both the leveraged loan and real estate markets are likely to be vulnerable to higher interest rates, whilst consumer credit expansion and the resulting high levels of personal debt may have left many consumers vulnerable to interest rate rises, especially after such a prolonged period of low rates.

Looking at the wider global economic picture, we see a mixed outlook. Economic growth continues to be strongest in parts of Asia although Chinese growth has slowed, while the outlook for emerging and developing economies is uneven. Recoveries in both the UK and US are now close to a decade long, while Eurozone expansion—although

Foreword

weaker—is also well embedded. Historically, downturns or recessions have occurred at least once each decade, suggesting that such an event may be overdue[3].

Some commentators consider that the global economy has reached its "late cycle" phase, most evident in asset valuations that appear stretched on historic bases. In the EU, close to €731bn[4] of non-performing loans continue to act as a major risk to some banks' resilience and profitability, while globally, increasing trade protectionism and political uncertainty also weigh heavily on the minds of many in the industry. Brexit continues to be a major geopolitical and regulatory uncertainty, and both regulators and politicians will attempt to mitigate its risks and effects throughout 2019. Nevertheless, if there is a disorderly Brexit, leading potentially to new political strategies and approaches, the implications for how a number of these regulatory predictions unfold in the UK could be profound.

Against this background, we expect regulators across sectors to remain highly vigilant to the risks of economic downturn and market shocks. They will likely want to use stress testing extensively to assess firm vulnerability and resilience, recognizing that during a period of unprecedentedly low interest rates some business models have grown up in relatively benign conditions and have yet to be tested in a sustained downturn.

A retreat from global coordination

The global regulatory approach is changing. The aftermath of the financial crisis saw a globally coordinated response to draw up a series of new regulations which would underpin a more robust and stable financial system. However, there is starting to be a move away from global policy making and a reduced appetite for cross-border regulatory cooperation. As a result, there are increasing signs of regulatory divergence, including geographical and activity-based ring-fencing, as different regions and countries look to tailor regulations to their own needs. Global firms are, therefore, having not only to comply with these divergent rules in the different jurisdictions in which they operate, but also to optimize their local governance structures, operating models, legal entity structure, and booking models.

A shift to supervision

We do not expect regulators to embark on a path to wholesale unravelling or reversing the post-crisis reforms implemented since 2008. But it seems that, absent a significant unexpected event, there is little prospect of major new regulation, especially in relation to bank and insurance capital. Regulators' key priorities are to consolidate and safeguard and—in some jurisdictions—refine the reforms of the past decade. What we do expect is a sharp tilt away from a period of regulatory re-design and innovation, to one of operating and embedding the reformed supervisory system.

As a result, firms in many countries are seeing rising supervisory expectations, reflecting the growth of principles-based supervisory approaches that emphasize the importance of firms' governance, culture, and management approach and the outcomes, both prudential

Foreword

and conduct, these are delivering. Firms' conduct and the treatment of their customers are also receiving increased focus in numerous countries, driven by political and regulatory concern over the perceived poor conduct of firms across all financial sectors[5].

Supervisors are also adopting more intrusive practices, including greater use of on-site supervisory visits. This reflects global leading practice and the increasing need for supervisors to engage directly with firms in order to understand their strategies and business models, risk profiles and appetites, risk management frameworks and approaches, and to hold boards and senior management accountable for the outcomes these deliver.

New technologies

Firms, regulators, and their customers are considering the opportunities and risks associated with new technologies. For example, due to the rapid development of artificial intelligence, machine learning, and fintech solutions, once new technologies are quickly becoming mainstream. The powerful impact these technologies will have should not be underestimated, not only on consumers, but also on regulation and supervision. The pace of technological change, therefore, demands deep thinking about the appropriate regulation of processes, products, and institutions to avoid regulatory gaps and to ensure financial stability and consumer protection.

These technology developments and disruption have triggered a debate around the perimeter of financial services regulation. Many incumbent firms worry that new technology-driven entrants offer services that lie outside the boundaries of existing financial services regulation, and which incumbent firms find more costly to deliver because of a "compliance leakage" from the regulated activities that they are undertaking. We do not expect regulators to come to the rescue of incumbents, who will have to look to their own resources to rise to the challenge of competition. However, we expect that these level playing field concerns, along with worries about the role of technology in society more generally, will drive increasing interest in how fintech firms and crypto assets are regulated—or rather, at present, how they are not. We expect clarification of the regulatory treatment of crypto assets, especially in the areas of investment by retail consumers, money laundering and prudential capital for banks.

Acting in the face of uncertainty

While the current regulatory environment appears more settled compared to the recent past, regulators across the world continue to set high expectations intended to maintain a strong, resilient financial sector through firms having robust financial and operational resilience, supported by strong risk management and compliance capabilities. In our view, this may provide an opportunity for leading financial firms to pivot from having to build frameworks to reflect a barrage of new regulations to optimizing through taking advantage of new technologies and operating models.

Foreword

The world changes and regulation changes with it

The debates around the regulatory perimeter and potential fragmentation of the financial system mean that firms' operational resilience, as well as their susceptibility to cyber and financial crime, are becoming a much greater issues for regulators. As part of this, we also expect a sharpening supervisory focus on how boards and senior management teams control the risks posed to them by their exposure to outsourced providers and other third parties.

The past decade has seen profound and lasting changes in the structure of the economy, employment, and society. The providers, consumers, and regulators of financial services are all changing. Aging populations and new millennial consumers are demanding different types of financial services and products, distributed in different ways. This changing and challenging background makes it essential to consider the future of regulation holistically, rather than in a piecemeal manner. All sectors and stakeholders have an important role here, and we hope that this year's outlook from our Regulatory Centres will both inform and stimulate this discussion.

Kevin Nixon
Centre for Regulatory Strategy
APAC

Christopher Spoth
Centre for Regulatory Strategy
Americas

David Strachan
Centre for Regulatory Strategy
EMEA

Canadian introduction

In a global economic environment where monetary easing and low-interest rates are slowly giving way to interest rate normalization, the Canadian economic position can be characterized as standing at a crossroads. According to Deloitte Canada's latest **Economic Outlook**, "Either strong economic growth will continue causing the economy to overheat and create inflationary pressures, or economic growth will slow to a more moderate and sustainable rate of expansion." Our analysis anticipates the latter scenario playing out.

Against this backdrop, the financial services sector is expected to continue along two paths: technological innovation, to generate growth through enhanced customer experience and product innovation, and an intense focus on productivity, operating leverage, and structural cost reduction. These dual drivers of innovation and optimization will generate the creative tension in which most financial institutions will be making decisions to underpin growth and strengthen risk management.

Concurrently, regulators are indicating a focus on consumer protection. In 2018, the federal government introduced a financial consumer protection framework, signalling an interest in much higher standards of expectation for whistleblowing, complaints, and oversight of consumer protection issues by management and boards of regulated institutions. The Canadian regulatory landscape has also been significantly affected by the November 2018 Supreme Court ruling endorsing legislation to create a unified, pan-Canadian securities regulator. While it remains to be seen what will result from that decision, it marks a potential turning point for Canadian securities law. The argument for a national regulator is that it will make the rules more consistent across the country, help regulators manage systemic risks, and improve enforcement[6].

With this lens through which to view the year ahead, we have identified issues within the following themes as those that will have the most impact on Canadian FIs:

- **Business model transformation.** Real progress will need to be made this year regarding the London Interbank Offered Rate (LIBOR) transitioning and Fundamental Review of Trading Book (FRTB) readiness. As the implementation deadline draws near, those who are more prepared for it will have a clear advantage.
- **Cyber.** In an age when hacking and data breaches have become so commonplace that they are almost expected, cybersecurity continues to dominate both the headlines and the regulatory agenda. Supervisors are broadening their oversight beyond the nuts and bolts of risk management programs, with breach reporting and risk and regulatory implications associated with cloud computing emerging as central themes.
- **Digital compliance.** As banks move forward with innovation programs, it's critical they establish and follow a progressive compliance program to keep both their consumers and their institution safe while they enable the business. In fact, digital compliance is becoming a true business imperative.

Canadian introduction

- **Financial crime.** Using digital technologies, criminals are perpetrating increasingly sophisticated financial crimes across channels, geographies, and industries. FIs, however, continue to rely on siloed, inefficient, duplicative, and rigid operating models for prevention and detection. FIs will need to establish a holistic and integrated approach that recognizes the new interconnected realities of financial crime.
- **Fintech.** The financial technology market is maturing, and traditional banks and fintech firms are teaming up to offer innovative services. At the same time, the fintech regulatory landscape is evolving with the announcement of the Global Financial Innovation Network (GFIN), which builds on the proposal by the United Kingdom's Financial Conduct Authority earlier in the year to create a "global sandbox." Among the participating regulatory bodies is the Ontario Securities Commission (OSC), which was the first Canadian regulator to create its own "sandbox" environment: the OSC Launchpad. The Canadian government's recently established advisory committee on open banking, coupled with the financial services sector's continued focus on payments modernization, indicates that Canada will evolve further.
- **Integrated data.** Data quality and availability are growing concerns across all aspects of risk management and regulatory compliance. To address these concerns, data quality and availability need to be an enterprise activity, with shared responsibilities and accountability across all three lines of defence.
- **Payments modernization.** Payments modernization promises to confer significant advantages to the Canadian economy. But along with these benefits comes new risk, most notably the heightened risk of fraud and increased stress on treasury operations. The time is ripe for FIs to determine how payments modernization will affect their risk profiles, and to develop a prioritized list of actions to respond.
- **Risk operating model transformation.** FIs are rethinking their risk and compliance activities to be more efficient, seeking ways to squeeze the leverage from investments and hunt down the duplication that has resulted from over-engineering. Firms are looking to optimize their risk management approach, harnessing the technology and business innovations occurring inside and outside their doors while maintaining safety and soundness.

With these themes in mind, I am pleased to introduce *Strengthening resilience: 2019 Canadian regulatory outlook for financial institutions*. This overview offers key insights on how the dual paths of innovation and optimization are increasingly imperative when addressing regulatory priorities and business demands.

Jay F. McMahan
Canadian Leader, Center for Regulatory Strategy
Canada

Business model transformation

Fundamental Review of Trading Book

Implementation and timelines

Fundamental Review of Trading Book (FRTB) is a globally applicable standard for measuring market risk in trading portfolios, introduced by the Basel Committee on Banking Supervision (BCBS) in January 2016. It was followed by a period of extensive consultation with the industry, and was finalized in January 2019. It will come into effect early 2022. European Union policymakers have recently signalled that banks may potentially be required to implement FRTB initially as a reporting requirement only, as early as January 2021.

FRTB in the EU context

Data published in autumn 2018 from the European Banking Authority (EBA) assessing the potential impact of Basel III reforms on EU banks underlined the importance of the European Union's forthcoming implementation of global regulatory standards the capital banks must hold against certain activities. One of the most immediate issues, from the European Union's perspective, is addressing capital requirements for market risk through the implementation of FRTB. Given the magnitude of the projected increase in capital, EU policymakers have now decided to proceed with a multi-step implementation approach that may be more complex than the international standards intended.

For banks active in the European Union, this has profound implications for their FRTB work, but may also present them with a significant opportunity to pursue FRTB implementation in a way that may better support their strategic and business objectives.

Recent developments in FRTB implementation

In the European Union, FRTB had first been proposed as part of the second Capital Requirements Regulation (CRR2) in 2016. In December 2017, the BCBS agreed to postpone the international target for implementing FRTB to January 2022. The BCBS then re-opened the FRTB framework in March with a consultation on some of its elements to allow for a more proportionate impact on banks' trading activities. Partly in response to these BCBS developments, EU negotiators chose to amend the market risk component of CRR2 to implement FRTB initially as a reporting requirement only.

Although CRR2 has yet to be finalized, the endorsement on December 4, 2018 by EU finance ministers on progress to date with the European Parliament signals that the European Union's adoption of an FRTB reporting requirement is now the most likely outcome.

This approach, if ratified by both the European Council and European Parliament next year, will leave the full implementation of FRTB until new legislation, which the European Commission will not, in our view, propose until mid-2020.

How the FRTB reporting requirement would work

To operationalize the reporting requirement and to reflect any changes made following the BCBS consultation, the European commission will adopt a Delegated Act by the end of 2019 modifying the FRTB framework in CRR2. This effectively means that the commission would use secondary legislation to complete the implementation of FRTB in EU law as a fully functional capital requirement, but only to be used for reporting purposes until new legislation makes it binding.

Fundamental Review of Trading Book

Under the CRR2 text, banks would be expected to begin reporting revised FRTB market risk weights based entirely on the new SA one year after the adoption of the Delegated Act (potentially as early as January 2021, a full year ahead of the BCBS implementation target).

Banks wishing to obtain Internal Models Approach (IMA) approval under the new reporting regime for certain trading desks could still seek to do so and could begin using these models three years after the adoption of the Delegated Act (i.e., in 2023). During this time, binding capital requirements for market risk would continue to be based on the existing CRR rules, so any reduction in risk weights resulting from newly approved CRR2 IMA models would not bring a capital benefit for the duration of the reporting requirement.

Banks that are eligible for the derogation for small trading books may be able to forgo the reporting requirement until a binding framework is put in place, but larger banks should now be planning for a two-phase FRTB implementation, with many of the operational requirements for implementation potentially needing to be completed by 2021 rather than 2022.

To bring FRTB fully into force as a binding capital requirement, the commission will need to make a new legislative proposal to this effect. Our view is that this will happen by June 2020 as part of the CRR3 legislative proposal.

As a result, between the time that CRR3 will take to negotiate (ending in mid-2022 at the earliest) and the time that FRTB is then likely to need in order to be implemented, it seems virtually impossible that the European Union can implement the binding FRTB standard by the BCBS's January 2022 target. Rather, a delay of at least two years past that point now looks difficult to avoid.

What does this mean for banks?

Banks facing the growing likelihood of a two-phase introduction of FRTB in the European Union now need to consider what this means for their implementation planning. This will be a challenge, as banks operating in the European Union may need to comply with an FRTB-based reporting requirement as early as 2021, but continue to face considerable uncertainty over the final shape and economics of the framework.

Banks that currently use IMA face the prospect of reporting significantly larger market risk weights during the first two years of the European Union's implementation, when reporting under the SA will be the only option available to them. Different implementation timetables and approaches between the European Union and the rest of the world will be particularly challenging for internationally active banks.

One decision of particular importance will be whether banks seek regulatory approval to use IMA models under the new CRR2 regime during the FRTB reporting period. Banks that do not seek IMA approvals during the reporting period may struggle to do so on time if they begin their work only after the CRR3 legislation is finalized, or may find themselves at the back of the queue for supervisors in their model approval work. A number of banking supervisors have indicated that the FRTB model approval process is likely to take several years.

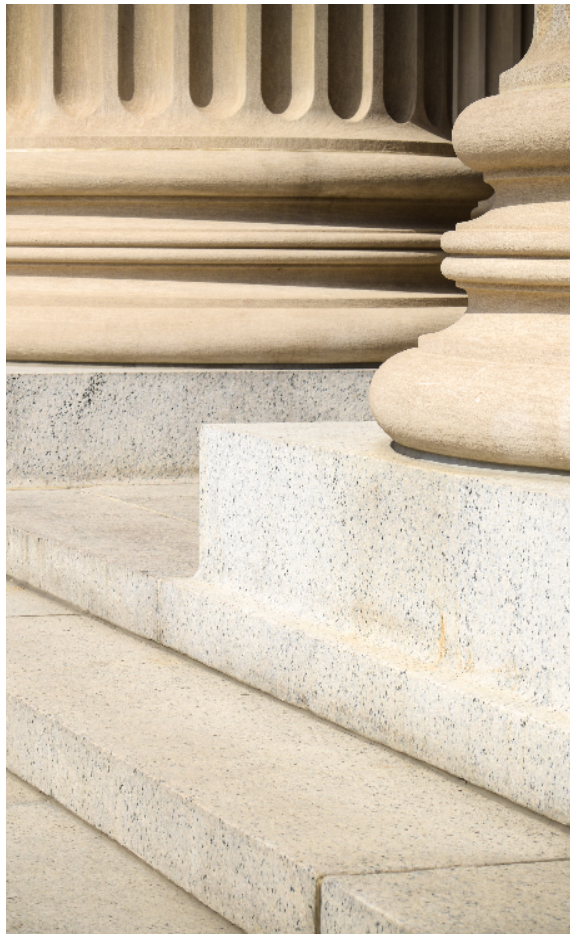
Fundamental Review of Trading Book

How will Canadian banks be affected?

Canadian deposit-taking institutions with capital market presence in the European Union should anticipate having to report capital under SA for their European Union subsidiaries by January 2021. Given that Office of the Superintendent of Financial Institutions (OSFI) has previously advised that the first regulatory reporting under the FRTB rules will commence no earlier than in the first quarter of 2021, recent developments in the European Union should not throw Canadian banks' delivery programs off-course. However, there are some implications that require senior management attention, including:

- The need to maintain two parallel operating models—SA FRTB and Basel 2.5—as well as separate Trading Book/Banking Book hierarchies and limits management frameworks.
- The inability to obtain IMA approval for the European Union-based desks until potentially 2023.
- For banks that haven't started their development yet, the news from the European Union effectively leaves them with only one year to complete all SA builds if one full year of testing is a target.

- **FRTB is about more than just the models; it affects the bank's whole strategy.** The FRTB affects front-office business practices more than any previous piece of prudential regulation. Desk-level approvals mean that the business will have a direct and daily interest in the performance of the risk models, while the impact on risk-weighted assets (RWA) is drastically redistributed across the desks.
- **A top-of-the-house strategic approach to capital analysis.** Our experience in capital impact analysis has led us to steer clients away from desk- and product-level standalone analysis, as this can prove misleading when portfolio diversification effects are taken into account.



Fundamental Review of Trading Book

Challenges

- The change in methodology for capital charge calculation may lead to higher capital charges and make certain products not economically viable, prompting banks to exit certain businesses. It may even have political implications; for example, for emerging markets.
- A conservative interpretation of the requirements, such as categorizing every unobservable risk factor as an individual non-modellable risk factor (NMRF), quickly leads to prohibitive levels of capital. Mitigating initiatives, such as finding a supply of adequate market data, could add significant time and expense to implementation.
- Calculations under FRTB rules, especially assuming a full revaluation approach for the IMA, place significant demands on the amount and granularity of data, and require a notable increase in computing power.

Key takeaways

- Although the EU's complex approach does inject more uncertainty into FRTB implementation, banks should nevertheless seize the opportunity to make strategic use of the extra time they will likely have before binding requirements come into force.
- Aligning many of the risk and data infrastructure upgrades that FRTB requires with a much clearer understanding of the stages in which the regulation will be rolled out could allow banks to pursue implementation in a way that supports their broader strategic, regulatory, and business objectives.
- Lack of technical clarification could result in widely diverging interpretations and RWA levels in the industry—which is precisely what FRTB was intended to avoid.

Insights to action

- FRTB implementation is a significant and costly undertaking, and should be used as the vehicle to streamline and enhance an institution's processes and technology capabilities that would be beneficial in the long run. Any opportunities to do so should be explored and included in the implementation plan.
- Participation in industry quantitative investment strategy (QIS) is highly advisable—the process of running a QIS serves as an effective test of the bank's readiness for go-live, as well as allowing for access to peer results.
- Given the impact of FRTB rules on desk structure and economic viability of certain product types, business stakeholders should be engaged early on and provided with information and tools to support capital impact assessment and decisions related to changes in business strategy.
- Align risk and data infrastructure upgrades required by FRTB with implementation stages to allow banks to pursue implementation in a way that supports their broader strategic regulatory and business objectives.
- Leverage FRTB implementation to align risk and finance functions more closely, to monitor market risk better on a daily and intra-day basis, and to enhance operational efficiencies throughout the traded risk process.

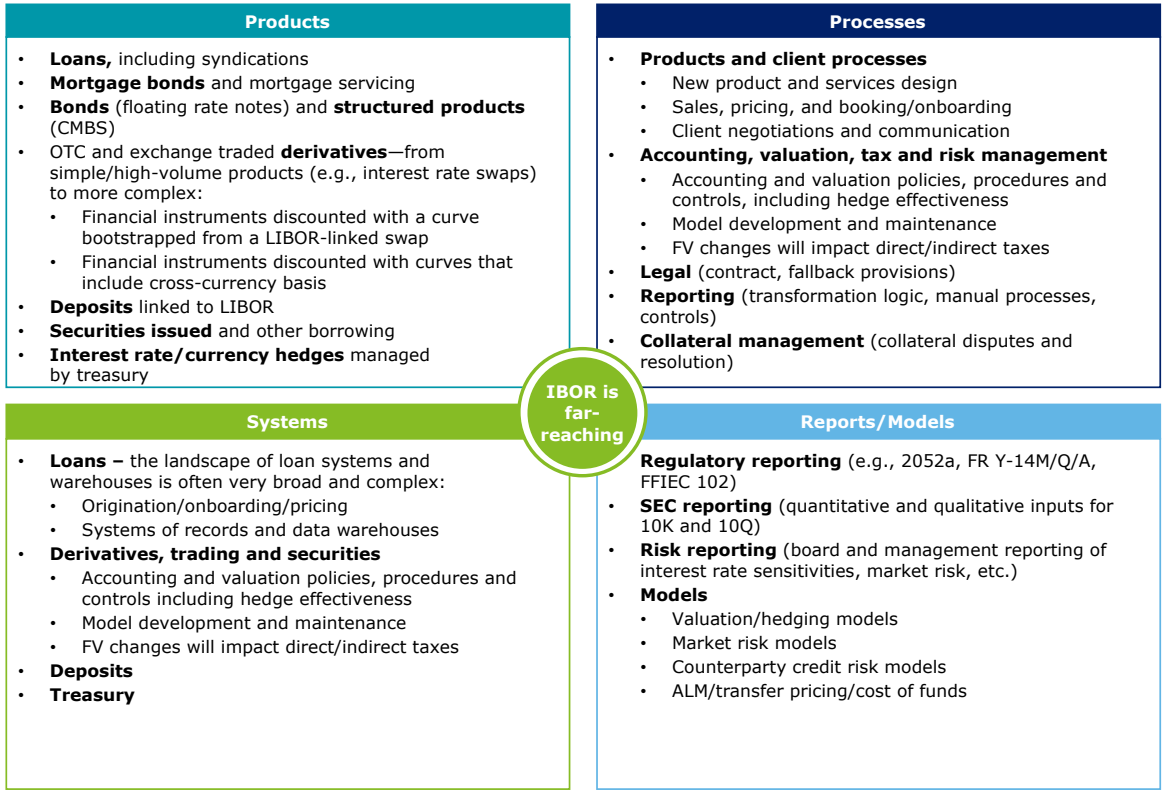
IBOR transition

Inter-bank offered rate (IBOR) transition. The London Inter-Bank Offered Rate, or LIBOR, is a key interest rate benchmark used in calculating floating or variable cash flows for loans, bonds, derivatives, and other financial instruments. Inter-bank offered rates, or IBORs, also exist outside the G5 countries.

In 2017, Andrew Bailey, chief executive of the United Kingdom's Financial Conduct Authority (FCA), announced that by the end of 2021, the FCA would no longer seek to persuade or compel panel banks to contribute to LIBOR. In July 2018, Bailey added that, "[…] firms should treat it [LIBOR transition] as something that will happen and which they must be prepared for."[7] Regulators globally have also clearly signalled that firms should transition away from IBORs to alternative overnight risk-free rates (RFRs).

Challenges

IBORs are widely used by banks, asset managers, insurers, and corporations. These rates are deeply embedded in the operational activities of the institutions using affected financial products, making the transition a highly complex task. This project is likely to be one of the biggest transformations firms will have undertaken.



IBOR transition

Key insights

We anticipate that in 2019 there will be an increase in activity as firms wake up to the fact that there is a significant amount of work to be undertaken. Regulatory and supervisory scrutiny is likely to grow across jurisdictions, with focused intervention in areas where tangible progress is not apparent. This is despite the absence of a formal regulatory or legal mandate to effect this change. Although there is a backdrop of uncertainty, and while firms may consider 2021 to be a long way off, there is no room for complacency.

IBOR impacts

The figure on the previous page identifies at a high level the impact of the IBOR transition on an FI. All lines of business must be considered, since there is a wide range of financial products that reference IBORs in their pricing or payoff profile. Products used for internal risk management purposes, such as hedges, also need to be considered.

Where are the markets?

The process to replace risk-free rates (RFRs) has begun in earnest. The Sterling Over Night Index Average (SONIA) rate, the RFR for the British pound sterling LIBOR, while in existence for some time, was updated in 2018. The Secured Overnight Financing Rate (SOFR) for the US dollar is being traded actively, while in Europe, the Euro Short-Term Rate (ESTER) will go live in late 2019. In Switzerland and Japan, the Swiss Average Rate Overnight (SARON) and Tokyo Overnight Average Rate (TONA) will replace the Swiss Franc (CHF) and Japanese Yen (JPY) LIBOR respectively. The Canadian Alternative Reference Rate Committee (CARR) has met quarterly since the FCA announcement and is formulating plans to replace the Canadian Overnight Repo Rate Average (CORRA).

Looking ahead

Real progress needs to be made in 2019. Boards need to establish a coordinated, senior steering committee to manage and oversee the transition and put in place the key activities and controls that will drive the program. Firms should expect regulators' questions on their financial exposures, readiness for the transition, and management of conduct risk. The largest firms will likely receive the greatest regulatory scrutiny, but all firms, including the buy-side, should review and understand the content of the FCA's "Dear CEO" letter and ensure that they position themselves to address the challenges. A clear client communication strategy, underpinned by rigorous program controls, documentation, and conflicts of interest management will be vital.

All the while, firms need to deal with a number of uncertainties, including the different construction of IBORs and RFRs, the lack of RFR term structures, and the cost of a program of this size.

To understand the financial impact, firms need to assess their exposure to all IBORs, including identification of contracts that require renegotiation, and to determine how they'll manage-and reduce over time-their exposures and vulnerabilities. Decisions should be made as to when to issue RFR-linked products to "make the market" (some have already done so) and discontinue their issuance of IBOR-linked products. Operational and systems changes will also be required.

IBOR transition

Moving legacy IBOR-linked products to RFRs could create winners and losers, with one party paying or receiving more, or less, because the methodologies for calculating RFRs are different. Conduct risk management is a crucial focus in transitions of this nature and firms need to be seen to be managing customer interactions appropriately. Firms that continue to issue IBOR-linked contracts that mature past 2021 or even in the run-up to 2021 will be increasing their exposure to IBOR and, as a result, the associated risks will increase. Firms need a clear strategy on when to stop issuing these contracts, and on regular monitoring and oversight of their exposures.

Insights to action

To move IBOR transition programs forward, FIs need to undertake the following proactive steps:

- Mobilize a cross-business unit and geography transition program with C-level sponsorship.
- Set out a transition roadmap based on a transition strategy. Plan all activities that do not have an external dependency.
- Identify the risks and implement mitigations early in the process.

Key take-aways

IBOR transition will be like no other transformation program. Boards should ensure that their programs have been mobilized, that they have a clear transition plan, and that they are actively managing them.

IBOR reform impacts on risk modelling under FRTB

Some firms have identified concerns that a lack of liquidity and observable transactions in either the new RFRs or legacy inter-bank offered rate benchmarks during the initial transition phase may cause some risk factors to become non-modellable. If these concerns materialize, the net effect could be a significant increase in capital requirements for the firms concerned. Firms have been approaching regulators to seek a carve-out in FRTB to exempt trades affected by the IBOR transition.

Cyber

Cybersecurity is a critical issue that's receiving regulatory attention from every direction.

In an age when hacking and data breaches have become so commonplace that they are almost expected, cybersecurity continues to dominate both the media headlines and the regulatory agenda. This includes reporting on the cost of cybercrime (and on the investments that organizations are making to enhance their cyber risk management programs), as well as a heightened focus on cybersecurity regulation and compliance.

With growing recognition of the importance of cyber risk management, supervisors are broadening their oversight beyond the foundational risk management programs—with breach reporting and risk and regulatory implications associated with cloud computing emerging as central themes.

Disclosure: Breach reporting

Canada now has mandatory privacy breach legislation in place at the federal level. Effective November 1, 2018, companies subject to Canada's privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), are required to record and report breaches of security safeguards.

As the cyber threat landscape and responding legislation evolves, so too must an organization's breach-response strategy. To effectively mitigate today's complex cyber risks, organizations must adopt a proactive approach that is seamlessly orchestrated and executed—one that transforms a multifaceted process into a single cohesive response.

To build this type of response strategy, organizations must coordinate the responses of their various functions, including legal, privacy, insurance, cybersecurity, and forensics. Working cohesively, these teams should be able to address the full spectrum of cyber risks their organization may face, including cyber incident management, evidence preservation, and breach response.

Cost of non-compliance

- Responding inadequately to a breach may lead to increased regulatory scrutiny (such as an investigation, audit, review of the entire privacy program, and sanctions), financial penalties (such as fines, lost shareholder value, or lawsuits) and reputational damage (through reduced customer trust, brand value, and revenue).
- Failure to comply will not be overlooked, and breaches causing significant harm—such as humiliation, damage to reputation or relationships, and identity theft—cannot be hidden. While businesses will be left to determine how quickly to report, report they must. They must also provide the privacy commissioner with a record of all security breaches upon request.
- The privacy commissioner has the power to post breach notifications, raising the risk of class-action lawsuits.

The silver lining

Although the stakes of non-compliance are high, the silver lining to establishing or enhancing an organization's breach response plan and broader privacy program includes:

- Increased competitive advantage by enhancing customer trust and loyalty, heightening privacy awareness across the company, and achieving greater efficiency among the privacy, security, information technology, and data governance functions.

Cyber risk

- Reduced risk through effective cybersecurity risk management.

Implications of cloud computing

Cloud computing is rapidly evolving. It allows data and applications to reside online, enabling users to access them through a web-connected device, forming a part of the extended enterprise. Considering that the cloud creates a separation between individuals and their data, there are inherent concerns over privacy and regulatory oversight.

Regulators have set out expectations in these areas: data protection, identity and access management, vendor management, audit, logging and monitoring, and governance and risk management.

Challenges

As more components of business become cloud-dependent, it becomes more difficult to ensure the risks previously identified and managed within the perimeter-oriented premises are still relevant and will be adequately managed in the cloud. The increasing use of cloud-based services has resulted in an increasing demand for assurance regarding controls over the systems underlying those services.

The regulatory environment

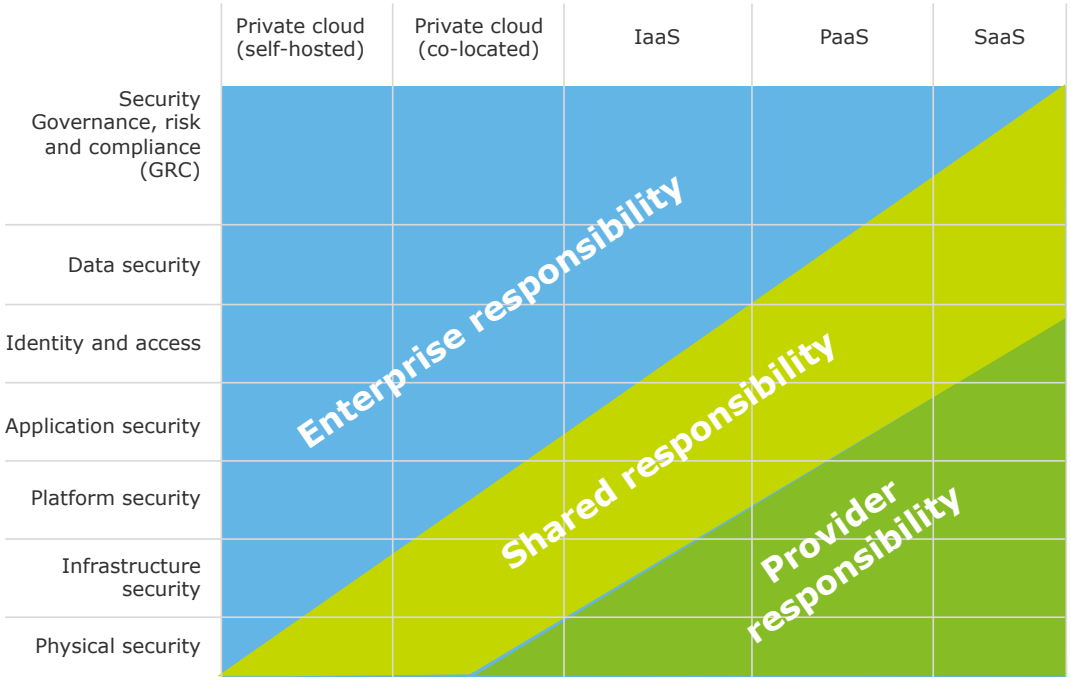
Regulatory guidance is still developing globally. No regulator in North America has forbidden cloud usage. In Canada, OSFI has not yet communicated a position on cloud computing; in the meantime, organizations are referencing OSFI's B10 outsourcing guidelines and using requirements and guidance issued by other jurisdictions.

Although regulatory requirements are still in development, enterprises need to be aware of current guidance and areas of risk and concern.

Regulatory requirements	Most regulators have issued guidance that indicates specific requirements companies should adopt in order to mitigate risks that cloud adoption brings.
Areas of risk and concerns	Regulators are mainly concerned about the following: data protection; identity and access management; vendor management; audit rights; logging and monitoring; governance and risk management; data location; data cleansing.
Participation in a regulatory program	Until standardized cloud-specific requirements are established (e.g., FedRamp), organizations will need to work with industry players, agencies, cloud service providers, and regulators to comply with high-level regulatory requirements.

Cyber risk

As FIs transition their business operations and applications to the cloud, which is managed by cloud service providers, cyber risk and compliance management become a shared responsibility between the FI and cloud service provider.



Insights to action

Cyber risk:

- Organizations should enhance the current risk management program to include a due diligence process/risk intelligence map, and policies and procedures to manage risks associated with cloud services.
- A cloud-computing framework should be adopted to define cloud delivery strategy, architecture, and sustainable operating model.
- Considerations should be taken to include "right to audit" and/or other contract/security compliance clauses within the cloud service provider contract to obtain assurance.
- A formal communication strategy with regulators should be developed to frequently communicate and demonstrate alignment with cloud-related regulatory guidance.

Cyber fusion

Given the change in today's environment of broad and evolving threats, fraud and cybersecurity functions need to collaborate to mitigate cyber threats. Past attacks have indicated strong links between the two and have shown that many fraud events originate from cybersecurity issues.

One emerging concept is to create a **cybersecurity fusion centre** that integrates functional teams from different parts of an organization. These teams have very diverse functional capabilities, including intelligence, forensics, operations, physical security, fraud, data science, and other related areas. Such teams are designed to create 24/7 situational awareness, rapidly share intelligence across the organization, and break down organizational barriers to take action, as well as act as a hub when dealing with crises. Fusion centre teams can also work across the wider ecosystem (partners, vendors, customers, etc.) to extend situational awareness. As a result, companies may realize faster and more efficient threat awareness with reduced costs and mitigation before, during, and following a breach.

Cyber fusion

Key takeaways

Adopting risk-intelligent leading practices, in conjunction with collaboration between fraud and cybersecurity functions, will be vital in the effort to promote security, privacy, and resilience in order to boost confidence in cloud adoption.

Insights to action

Cybersecurity fusion centre:

- Converging people, processes, technology, and data across domains such as cyber, fraud, and AML will provide increased visibility to predict, prevent, and detect cross-channel attacks.

Governance:

- Each function (cyber, fraud, AML, corporate security, etc.) should continue to own and operate its existing mandate; however, representation from each function should reside in the fusion centre (resource rotation between function and fusion centre).
- The leading practice is to establish a financial crime steering committee (with representation from each function) with a fusion centre director (new role) to ensure the success of this collaborative/cross-functional effort.

Processes/capabilities:

- Processes/capabilities specific to each function (case management, identity resolution, investigations, etc.) should continue to be followed with the aim of integrating/aligning/converging some processes to enable cross-function threat detection more actively.

Data/technology/facilities:

- Identify specific data elements from each function that can aid in developing fusion centre scenarios.
- Implement solution to forward selected data fields to fusion technology stack.

Technology/facilities:

- Establish a common war room in the fusion centre for collaboration and innovation.

Digital compliance

An emerging concept

With the digital revolution, society has witnessed the evolution of analogue, electric, and mechanical devices to the digital technology available today. While technological innovation, including digitization, has seen unprecedented growth in FIs, a digital compliance function is still an inspirational goal for most FIs. In this outlook, digital compliance is considered a broad term describing the use of technology to enhance compliance practices. This could have an impact across talent, process and controls, data, and infrastructure. Currently, organizations are still in the early stages of applying digital compliance practices sustainably.

Businesses are moving ahead. Can compliance keep pace?

FIs are increasingly adopting artificial intelligence (AI) and machine learning (ML) in their business and decision-making processes. In 2018, FIs collaborated with AI institutes, invested in AI research, and acquired or invested in AI companies. The capabilities that AI brings to the bank will be intertwined with the development of all other technological innovations. In August 2018, the World Economic Forum and Deloitte Global released **The New Physics of Financial Services,** the report from their joint study of the strategic, operational, regulatory, and societal implications of AI on the financial services industry. The report found that AI is changing the physics of financial services, weakening the bonds that have held together the component parts of incumbent financial institutions, and opening the door to entirely new operating models.

As banking moves forward with innovation, it is critical to have a progressive compliance program to keep the consumers and the bank safe while supporting business enablement. While digital compliance has become an increasing business imperative, rarely has there been a dedicated investment for this strategy. This inertia is a symptom of a broader dearth of innovation in compliance risk management. As digital banking proliferates, the pace of progress may be hampered by the inability of the bank's second line of defence to be responsive to the changing environment.

Trailblazers

A small but growing number of organizations have been experimenting with digital technologies to enable their day-to-day compliance processes. Their experiences serve as case studies for other firms looking to move forward with developing their digital compliance functions. Based on the case studies that Deloitte has been gathering for analysis, digital compliance is showing the most potential in the following applications:

- Business decision and process management to embed compliance controls to transaction systems for real-time decision-making.
- Automation, robotics, and advanced analytics for monitoring and testing practices.
- Enhanced documentation review, such as Deloitte Intelligent Contract Execution (D-ICE) that combines optical character recognition software with ML and natural language processing (NLP) to review marketing and disclosure documents against regulatory expectations. It can deliver improved efficiency and quality across a wide range of use cases.

Digital compliance

Chief Compliance Officers (CCOs) may choose to invest in or undertake one or all of these initiatives. Collaboration between CCOs, Chief Operating Officers (COOs), and others from the executive team will be important in identifying the compliance practices that would benefit most from digitization. More value will be derived from considering a digital compliance function from end to end across the first and second lines of defence. Much will depend on the bank's existing strategies, capabilities, and requirements as well as on current technologies and skill sets.

Benefits

Early adopters who have embedded compliance requirements (in front-line digital processes, transaction systems, etc.) have seen significant benefits, such as:

- Facilitating real-time decision-making.
- Instant identification of non-compliance and prevention of potential compliance issues.
- Cost reductions, by automating repetitive manual activities (e.g., accessing multiple products and know-your-customer source systems using robotics).
- Seamlessly integrating compliance in the customer experience.
- Enhancing the effectiveness of monitoring and testing processes using automation, robotics, and advanced analytics.

The regulatory landscape

Managing risk innovation is top of mind for FIs and regulators alike. Because AI and ML applications are relatively new, there are no known dedicated international standards in this area. More progressive regulators are embracing advanced technologies and expecting FIs to evolve and adapt. For example, the Monetary Authority of Singapore announced a progressive roadmap to reduce data duplication and automate data submission by FIs.

Key messages

- Business and compliance should partner to embed regulatory compliance requirements in front-line digital processes and automatically monitor ongoing compliance. Those who work together, while supporting their mandates in parallel, are more likely to be successful.
- It is important to have the right talent to help with the change. This may require a talent transformation so that the compliance talent profile supports digital capabilities. This includes employing tech-savvy compliance professionals who understand emerging technologies and partnering them with compliance subject matter experts to enable job shadowing and knowledge sharing.
- The focus on digital compliance is not just on automating processes and procuring the latest technology to enable it. The organizations that do it right will also focus on the capabilities of their resources, and levelling them up to be more digitally aligned. For example, this could mean providing better hardware/software for employees (e.g., tablets or analytics tools) to encourage collaboration and an iterative delivery mentality.
- Compliance must ensure they have the appropriate capabilities in place to execute on their oversight mandate

Digital compliance

in an environment where businesses are adopting emerging technologies. For example, the capabilities required to provide independent compliance oversight over highly manual processes may potentially be very different from the capabilities required to provide independent compliance oversight over an AI-driven solution.

- Compliance, as best it is able to, should track benefits to show the value/return on investment. If compliance is not able to track the return on investment, it should ensure another group can track and report this information on its behalf.

Key takeaways

The use of technology to manage regulatory compliance enhances the effectiveness of compliance risk management and improves operational efficiency. This should lead to long-term operational savings and compliance issue prevention.

Insights to action

- A strategic roadmap can help make digital compliance a reality. Determine the desired state of digital compliance.
- Focus on improving procedures that use structured, rule-based processes, where technology can automate routine tasks allowing compliance professionals to focus on more complex issues and exceptions management.
- As FIs set out on new digital compliance journeys, supported by Big Data/AI applications, they will need to understand how the use of these technologies affect their overall risk profile.
- A dedicated effort should be made to move the dial on digital–if this is a side-of-the-desk exercise for your top performers, the vision will not be realized.
- Actively work with your first line to develop streamlined digital compliance processes–advancements in technology mean that first and second line processes and controls can be seamless.
- Compliance will need access to good quality data. A critical factor will be the ability to pull data from numerous sources and then aggregate it to get a fulsome view. AI will only be as useful as the data driving its algorithms.

Financial crime

The pressure to tackle financial crime has never been greater. Using digital technologies, criminals are perpetrating increasingly sophisticated financial crimes across channels, geographies, and industries. Some FIs, however, continue to rely on siloed, inefficient, duplicative, and rigid operating models to detect and prevent financial crime, resulting in sub-optimal performance and, in some cases, penalties and fines. FIs often lack a holistic, single view of the customer across products, channels, and geographies. It is becoming increasingly complex to manage financial crime risks as criminal methodologies evolve, new technologies heighten customer expectations, and new regulations raise the cost of compliance. To avoid falling behind, FIs need to recognize the continuous reputational risk they face and reconsider their approach to mitigating financial crime.

Risks from increased digitization

Despite the advantages made possible by digitization, these new technologies present FIs with nascent forms of risk. In addition to raising consumers' real-time expectations and driving increased competition among FIs, digitization necessitates the management and monitoring of vast and growing amounts of data. Furthermore, digital technologies also provide criminals with increasing entry points to banking, thus creating more opportunity to perpetrate financial crimes. Institutions are also faced with the risk of insiders enabling external threat actors, whether knowingly or not.

Challenges

Despite this changing landscape, most FIs continue to rely on outdated risk management mechanisms. Their current siloed operating models are often the result of reactive changes introduced in an attempt to keep apace with new regulatory requirements. This has resulted in financial institutions managing financial crimes with multiple teams, each relying on diverse tools, technologies, and reporting structures, thus making it challenging to share information optimally across the entire organization.

How will financial institutions respond?

Given these significant challenges, many FIs are contemplating the extent to which they want to be seen as market leaders in protecting customers from financial crime while simultaneously finding the most optimal approach to achieving their desired outcome within their current operating environment. Many financial institutions are looking for the most cost-effective way to reset their business model and organization to minimize vulnerability and protect customers while managing their bottom line.

The way forward

The way forward is simple in concept: establish a holistic and integrated approach that recognizes financial crime is now interconnected and spans product suites and channels. However, creating an infrastructure that addresses financial crime is exceedingly complex in reality. It involves a shift to an integrated framework with a single, unified operational capability that is both agile and adaptable. This framework involves integrating data and systems to gain an enterprise-wide view of identity and risk, developing a standard language for defining financial crime across the bank and the various typologies of risk it faces to allow for effective identification, classification, and measurement. The framework should also include a common technology platform and advanced analytics to allow for real-time decision-making and proactive threat detection.

Financial crime

Opportunity in the face of challenge

Adopting an integrated, shared services approach may yield benefits across the enterprise, including:

- Ability to protect both the customer and the bank from financial crime risk, given new realities.
- Alignment of objectives and mandates with respect to crime across financial channels, with clear roles and defined accountability.
- Economies of scale and an overall reduction of operational costs through automation and reduced duplication.
- A holistic customer view and improved customer experience.
- Better information sharing across the organization through the use of a single data repository.
- Strengthened financial crime insights and clearer mitigation actions.
- Enhanced efficiency levels through the adoption and use of advanced data analytics and digital technologies.
- Proactive threat detection across a unified platform, allowing financial institutions to better protect themselves and their reputation.
- Improved loss containment and fraud reduction.

Key takeaways

Current trends suggest the threat and impact of financial crime will only accelerate, making resilience in the face of financial crime a critical imperative for the long-term success of any institution. A new, integrated approach is needed to address these risks and protect both the reputation of the bank and the customer.

Insights to action

To prevent and mitigate both internal and external threats to the bank while also delivering an industry-leading customer experience, FIs should implement a holistic approach to financial crime management that aligns roles and responsibilities across a centralized, shared services model. This includes:

- The integration of cybersecurity, internal and external fraud, and anti money-laundering (AML) functions.
- The ability to see financial crime through a digital lens in real-time, which more effectively—and proactively— capitalizes on technology and advanced analytics.

These initiatives are the first steps toward a financial crime unit capable of handling the threats against financial institutions and their customers.

Fintech

How to navigate the shifting regulatory landscape as the fintech (financial technology) market matures.

New investment in fintech firms remains strong, and the number of acquisitions and financial services partnerships are on the rise. This reflects a maturing financial technology market, where traditional banks and fintech firms are teaming up to offer innovative services. Traditional banks recognize the advantages of innovative and competitive technology to meet their customers' demands, while fintechs recognize the benefits of infrastructure and capital that is derived from such partnerships.

Two important developments in the United States' fintech regulatory landscape occurred in late July 2018, when the Treasury Department issued a report entitled ***A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation.*** It outlined core principles and recommendations for a fintech regulatory framework. A key recommendation was for the Office of the Comptroller of the Currency (OCC) to move forward with the national fintech charter. On the same day, the OCC announced it would begin accepting applications for special purpose bank charters for fintech firms that offer bank products and services.

Later in the summer, as a signal of the increasing interest in supporting a more efficient way for fintechs to interact with regulators, 12 regulators from around the world announced the formation of the Global Financial Innovation Network (GFIN), building on the proposal of the United Kingdom's Financial Conduct Authority earlier in the year to create a global sandbox. Among the participating regulatory bodies is the OSC, which was the first Canadian regulator to create its own sandbox environment in 2016: the OSC Launchpad.

In a 2018 report, Deloitte outlined the changing landscape in the fintech industry in the United States.[3] The report found that the number of new fintech startups rose from 177 in 2008 to 668 in 2014. However, in 2015, the rate of fintech formations began to decline, and was down to only 41 startups in the first nine months of 2017. In the banking and capital markets fintech category, the peak of 281 startups occurred in 2012, declining steadily to only 10 in the first nine months of 2017. The industry appears to be maturing and competition among fintechs themselves is causing some players to exit the industry, while giving pause to others considering entering it.

Despite the decline in new startups, new fintech funding remains strong in the United States—with a shift toward later-stage investment in a maturing market. At the time of the report, more than 2,000 firms were operating in the areas of banking operations, capital raising, financial management, deposits and lending, and payments. Acquisition activity is on the rise, with about 50 acquisitions occurring in the banking and capital markets category during the first nine months of 2017.

For traditional banks, fintech companies can represent either a competitive threat or an opportunity to offer better services and improved processes through strategic partnering. Many banks have embraced the latter, partnering with or acquiring fintech companies to modernize their own operations and services.

Fintech

While the OCC announced it is ready to start accepting applications in the United States for special-purpose bank charters for fintech companies, there is no requirement for any US fintech firm to seek a national charter. Yet, applying for such a charter from the OCC might be worth considering—especially for fintech companies operating in multiple states. However, the promise of greater consistency in regulation could come with downsides, depending on a fintech's business model. These downsides could include more burdensome regulatory requirements, and initially, a legal challenge from the states, many of which oppose the OCC's fintech charter.

The OCC defines a special purpose national bank (SPNB) as a "national bank that engages in a limited range of banking or fiduciary activities, targets a limited customer base, incorporates non-traditional elements, or has a narrowly targeted business plan." The OCC fintech charter is a subset of that. Chartered fintech companies can engage in the core banking activities of paying cheques and/or lending money, but cannot take deposits and will not be insured by the Federal Deposit Insurance Corporation (FDIC).

Alternatively, for other fintech companies, there could be great benefits in partnering with banks to capitalize on each entity's unique advantages and capabilities. Combining strengths has the potential to create more value than either business could produce on its own.

Banks and fintech companies should seek to understand each other's capabilities and needs by attending industry forums and roundtables that bring traditional banks and fintech firms together. They should also stay abreast of regulatory developments related to fintech firms and partnership arrangements, constantly looking for ways to enhance their services by partnering, or possibly merging.

In Canada, the fintech landscape varies from that of its southern neighbour. While Canada provides a fertile ground for fintech development, obstacles may prevent fintechs from maturing and realizing their full potential. Canadian fintechs have not grown at the same scale as their American peers, and lag in adoption due primarily to four main factors:

- The relatively low impact of the financial crisis prevented the shakeup of business models that allowed fintech to flourish in other countries.
- The higher level of trust in the financial sector due to the quality, breadth, and sophistication of its FIs resulted in consumers being less motivated to seek out alternative solutions and providers.
- The financial services sector is both relatively small and competitively intense, decreasing its importance as a strategic market to fintechs considering expansion.
- The current regulatory framework in Canada has been seen as a barrier to fintech adoption. (And to date, Canadian regulators have not focused on encouraging innovation.) For example, while American companies introduced peer-to-peer lending models that found traction, a similar offering in Canada was unable to operate effectively within the regulatory framework of the OSC.

Fintech

Nevertheless, the Canadian fintech sector continues to evolve, especially with respect to AI; in fact Canada is seen as a global leader in AI innovation. The year 2018 saw FIs collaborating with AI institutes, investing in AI research, and acquiring or investing in AI companies.

Key takeaways

As financial services regulation continues to develop—for example, the Canadian government's advisory committee on open banking, coupled with the financial services sector's continuing focus on payments modernization—it is likely the trend of increased activity in the fintech sector will continue.

Insights to action

- For legacy FIs, fintechs are likely to continue concentrating on value-chain segments where the greatest source of customer inconvenience meets the largest profit opportunities.
- Fintechs with the greatest chance of success will likely be those with the greatest ability to make use of customer data across platforms and that do not require onerous amounts of regulatory capital.
- The intersection of advanced analytics, consumer protection demands, the trend to open banking, and AI may create conditions that accelerate the transformation of business models and create new sources of revenue.
- FIs must embrace these drivers and develop their own vision of their strategic value to their customers in order to seize the opportunities that the combination of these forces will generate.

Integrated data

A framework for improving the quality, integrity, and availability of data.

Data quality and data availability are growing concerns across all aspects of risk management and regulatory compliance. To address these concerns, data management and data quality can no longer be the sole responsibility of the corporate functions or specific executives such as the CFO, CRO, or CDO. Instead, they should be an enterprise activity, with shared responsibilities and accountability across all three lines of defence.

Data owners within the FI should be asking: Is the quality of the data fit for the purpose? Are the origins of the data clear and well documented? Are data definitions and standards established and consistent across the enterprise?

Recently, some reporting requirements have been reduced through regulators' burden reduction efforts, regulatory relief legislation, and tailoring of data requirements. However, these reductions do not change regulators' expectations for managing data. Some of the reductions in reporting have been offset by new data requirements, particularly for large complex firms, and there is a general trend toward requiring more granular, product-level data—with more frequent availability. This trend underscores the need for strong enterprise data management practices and accountability.

Regulatory expectations for a firm's data environment currently focus on three areas:

- Strengthening governance and oversight.
- Building data competencies across the firm.
- Establishing an integrated approach to data.

This framework is applicable not only to regulatory reporting, but also to all data initiatives, including public reporting, liquidity management, risk management, and management reporting.

Strengthening governance and oversight

The banking industry is shifting and developing its approach to data-related governance and oversight. As practices mature, leading FIs are assessing how their data management processes align with their organization's operating model. The objective of a governance and oversight framework is to develop, communicate, and monitor effective data standards and policies. These standards and policies are the foundation for implementing an effective data environment. A critical element is having consistent data definitions and data quality standards. Another essential element is having a methodology for determining critical data elements (CDEs), which requires a firm to understand the origins of data, all downstream uses of the data, and the impact on all data users (including external parties).

In many cases, the most significant challenge FIs face in this area is the need for a culture shift. Effective firm-wide data programs require support from senior management and the board. Without a culture shift and top-level support, the key components of the governance process—and accountability of key stakeholders, including business lines—will likely not be achieved.

Effective oversight and accountability require a measurement and monitoring function armed with quantitative measures of data quality. These measures can be used to rationalize

Integrated data

and enforce accountability at the data owner/business line level. The monitoring function should also be responsible for aggregating and tracking data issues related to both quality and availability—ideally, managed through a single, centralized system. Data issues should be reviewed from a firm-wide perspective to identify any systemic issues, and to escalate issues based on their associated risk.

Data quality controls

Part of an effective data governance structure is having controls in place to ensure the integrity of data. Data quality programs are not a single responsibility or action. Effective programs include an independent quality assurance function that conducts detailed, end-to-end testing on a multi-year planning schedule that considers the impact of CDEs overlaid with a risk assessment. Effective data quality programs also include cross-dataset reconciliations. These reconciliations are a valuable tool for identifying systemic data issues and ensuring data completeness.

Building data competencies across the firm

With the heightened attention to data quality and the increased need for granular product-level data, the responsibility of data owners (usually residing in a business line) for data quality has intensified. To meet regulatory expectations, business lines, the finance function, and other data aggregators need to have expertise in data management and data analytics.

In many cases, data owners understand their data as it relates to their specific business, but have a limited understanding of how their data affects other users across the firm. Thus, the first step for business lines is to gain awareness of the firm's existing data standards and data programs. Formal awareness training is important for senior management and for all staff involved in providing data to the rest of the firm. Awareness training—which varies by role—helps data owners understand how their data is being used by others in the firm.

As data requirements become more complex, there is an increased need for specialists who can properly interpret how regulatory requirements relate to a firm's products and transactions. To address this issue, data owners and report owners (i.e., the functions responsible for reporting) need access to a pool of talent that understands capital requirements, liquidity management, and broad regulatory definitions.

Establishing an integrated approach to data

Historically, business lines have often maintained separate data and IT architectures. However, this siloed approach is no longer sufficient to meet regulatory expectations or the data needs of today's businesses. Sustaining a highly effective data program requires an integrated approach that includes finance, regulatory, risk, and capital data.

As data requirements continue moving toward more granular, complex data elements, the need for tools to analyze and validate the data also increases. Integration improves access to data across the firm. It also makes it easier to apply data analytics and AI technologies to data sets, enhancing the firm's data capabilities and process efficiencies. This is particularly important for product and transaction data with a large number of data attributes.

Integrated data

Key takeaways

The evolution of data practices in banking will continue to be influenced by the growing need for granular product-level data. When planning or conducting data remediation efforts, FIs should consider migrating to more mature practices that can improve data quality, integrity, and availability.

Insights to action

- FIs need to challenge legacy obstacles to integrated data management. The shift to an integrated data environment should be supported by a firm-wide data stewardship program, spanning:
  - Customers
  - Business lines
  - Products
  - Legal entities
- This program requires expertise in data management practices, structures, and organizational cultures that can look and operate beyond strict hierarchical structures.
- FIs should focus on innovation strategies that promote a culture of fail fast and learn quickly to help unlock potential value using more experimental methods.
- FIs must understand the barriers to the development of personalized products and services to help unlock greater customer engagement, retention, and trust.

Payments modernization

Background

In recent years, countries around the world have been moving to upgrade their aging legacy systems to enable faster payments processing, real-time settlement, and data-rich transactions. In 2016, Canada joined the mission with plans to build a new core clearing and settlement system, establish a real-time payments capability, enhance automated funds transfer, align with global regulatory standards, and modernize the rules framework. The vision is to create a modern payments system that is fast, flexible, and secure to promote innovation and strengthen Canada's competitive position.

The risks and rewards of real-time

While the benefits of this initiative are considerable for consumers, businesses, and government agencies, FIs stand to gain as well. After all, a modern payments platform promises to do more than make payments easier and faster. It will also deliver more robust analytics—providing FIs with greater insight into individual and organizational spending habits, enhancing their ability to improve capital and liquidity management, and positioning them to introduce more responsive products and services.

However, payments modernization is not without its risks. Concerns that the industry, Payments Canada, and regulators will not be able to collectively execute the payments modernization plan—due to its scale, scope, and speed—are raising a number of delivery risks. For instance, competing priorities, skills shortages, and capacity constraints may prevent the industry from reaching the target state on time, potentially increasing costs and risks. Growing reliance on new technologies could complicate execution, particularly if they are not compatible with the systems that currently process critical payments. Aside from execution risk, this could lead to customer confusion, service disruptions, system failures, and widening gaps in risk management oversight.

New risks also abound as the industry works to reach the initiative's target state. Risks include the potential inability of banks to proactively measure how much incremental risk they will incur due to the threat of increased fraudulent activity, additional cybersecurity exposure, and higher collateral requirements. Together, these risks create challenges for FIs to maintain the safety and soundness of the financial system, particularly in the early stages of implementation when the risks of system disruption and potential data loss are likely to be highest.

Implications of payments modernization

Along with the myriad benefits associated with payments modernization come some weighty implications for FIs. The two most notable of these are the risk of fraud and the stress on treasury operations.

1. Risk of fraud

When the United Kingdom launched its faster payments system in 2008, fraud losses from online banking rose by almost 300 percent—from £22.6 million in 2007 to £59.7 million in 2009.[8] If a bank isn't fully prepared at inception, it could experience a snowball effect of fraudulent activity that is harder to deter once initiated. It is apparent that some of the key benefits of real-time payments are also its main weaknesses, such as:

- **Speed.** Real-time payments happen so quickly that banks have little time to conduct fulsome fraud monitoring.

Payments modernization

- **Irrevocability.** With the Lynx system, which will be replacing the Large Value Transfer System (LVTS) and real-time rail (RTR), payment transfers between Canadian FIs become irrevocable once they are authorized.

- **Proxy identifiers.** To meet evolving customer needs, Canada's new payments infrastructure proposes to use additional proxies—mobile IDs, emails, phone numbers—to identify customers and enable them to make payments. While this will deliver unprecedented payment flexibility, it also heightens security concerns and risk of fraud.

- **Higher transaction limits.** Daily Interac e-transfer limits currently sit at $3,000, but that is set to change. With payments modernization, daily transaction limits may start at $10,000 and potentially reach or exceed $100,000. By presenting cybercriminals with more lucrative opportunities for fraud, these higher limits may lead to higher losses.

- **Data-rich transactions.** Payments Canada is proposing the introduction of a global messaging standard with expanded memo capability. These data-rich transactions will increase the risk of exposure to malware, which could be embedded in payment attachments or links.

Responding strategically

A bank needs a lead time of one year to 18 months to adequately prepare for the heightened risk of fraud. FIs will need to ensure that practices and processes circumvent this risk by:

- Introducing real-time fraud detection and prevention capabilities that use advanced analytics to identify fraudulent patterns as they arise.

- Strengthening authentication procedures.

- Protecting all channels and payment types equally.

- Monitoring both outgoing and incoming payments.

- Enhancing cybersecurity systems to prevent cybercriminals from using advanced tools to attack systems or insert malicious code into a transaction's rich message field.

2. Stress on treasury operations

There is little doubt that Payments Canada's modernization initiative will facilitate faster funds transfer and more efficient settlement. Yet the new platforms and rules that will enable these outcomes are set to take a toll on FIs' treasury operations. Specifically, banks will need:

- Significant increases in collateral requirements.

- A new approach to intraday liquidity management.

- Data and technology upgrades.

Responding strategically

As the modernization initiative progresses, FIs will need to take steps to mitigate these emerging risks. Although no one-size-fits-all solution exists, banks may want to:

- Enhance collateral management to improve collateral monitoring, reduce financial risk, and streamline their systems in a way that optimizes compliance with the Lynx, Settlement Optimization Engine, and RTR collateralization rules.

Payments modernization

- Assess and revise intraday liquidity models to gain active visibility into liquidity reserves, improve their liquidity forecasting, and adopt appropriate liquidity saving mechanisms.
- Review existing technology system capabilities to pinpoint potential gaps and identify any upgrades needed to meet the added monitoring and reporting requirements introduced by payments modernization.
- Analyze how new collateral and liquidity processes may affect regulatory compliance by altering financial ratios, and adopt early-warning indicators to avoid falling offside.

Key takeaways

- Payments modernization promises to confer significant advantages to the Canadian economy. Yet along with these benefits come new risks—ranging from increased collateral requirements, greater strain on liquidity models, and the need for technology upgrades to combat elevated threats of fraud and cyberattack.
- The time is now ripe for FIs to determine how payments modernization will affect their risk profiles and develop a prioritized list of responses. The key will be to approach payments modernization not simply as a compliance exercise, but also as an opportunity to strengthen risk models, optimize liquidity and payment processes, and improve customer satisfaction through the adoption of more robust and secure technologies and systems.

Insights to action

- It is essential FIs take the time now to plan how they'll ensure criminals are deterred from the first day of real-time launch.
- FIs need to ensure they have strong authentication capabilities across all channels.
- FIs need to prepare in advance for the intraday liquidity and collateral changes that will come with payments modernization. Specifically, banks will need:
  - Increases in collateral requirements
  - A new approach to intraday liquidity management
  - Data and technology upgrades
- FIs need to respond strategically to the significant implications of payments modernization. With swift action, they can likely realize cost savings that will be harder to gain as implementation deadlines get closer.

Risk operating model transformation

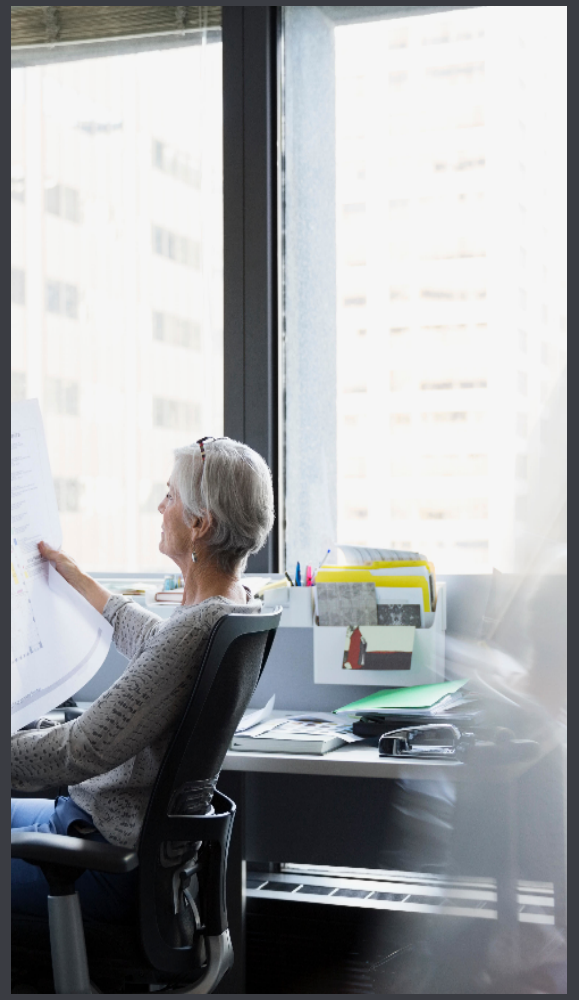
Improving the efficiency of risk management systems while maintaining safety and soundness by capitalizing on the latest technology and process innovations.

Overview

Risk management is at an inflection point, with competitive pressures and emerging technology developments challenging conventional orthodoxies of risk management.

- Regulation has become both a driver and a constraint of business strategy, capital, liquidity, corporate behaviour expectations, risk infrastructure requirements, and cost.
- Despite massive spending to meet these requirements, risk management is often not fully meeting stakeholder expectations.
- Simultaneously, the market has developed new delivery models and capabilities that offer the possibility of a transformative risk environment.

These events offer the opportunity to redefine an FI's risk operating model. FIs want risk and compliance activities to be more efficient, and are looking to eliminate the duplication that resulted from over-engineering, specifically with regard to the three lines of defence model. However, while firms seek to optimize their risk management approach by harnessing technology and business innovation, consumer protection and conduct risk management have simultaneously risen on the priority list of regulators and legislators.



Three lines of defence

Ten years after the financial crisis—and eight years after the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act—many firms have completed or nearly completed their build of new risk management systems, and they are now ready to truly return to business as usual. However, while intensive work has been completed, much has changed with regard to their customers, the marketplace, technology, and the regulatory environment since the blueprint of those systems was initially conceived.

Prior to the financial crisis, risk and compliance systems were heavily siloed, and the operating environment was characterized by highly manual processes, fragmented controls, and a check-the-box mentality. Afterwards, given the heightened expectations of Dodd-Frank reform and regulators' low tolerance for missed deadlines and inadequate solutions, systems were built quickly and with a focus on sturdiness, not efficiency. FIs are now looking to optimize their risk management approaches and systems to be increasingly automated, flexible, capable of near real-time risk reporting, and more closely linked to firm strategy and risk appetite—and they're harnessing the technology and business innovations occurring inside and outside the institution.

To do this properly, FIs must look at the three lines of defence in aggregate in order to understand how the model is currently operating and the relationship between the three lines. Embedding a culture of awareness and reciprocal support will drive the optimization of the model. This culture can only be achieved if it's set by the tone at the top.

Where closer examination of end-to-end processes is conducted, more FIs acknowledge that there are unproductive redundancies in certain areas, and that controls are not always located in the right place to be both effective and efficient. For example, some firms are now moving selected testing and monitoring activities up to the first line of defence, with the goal of improving detection, prevention, and accountability. This move enables the second and third lines to conduct a more strategic review, while also freeing up resources for advanced data analytics, risk aggregation, and targeted testing to evaluate risk better.

Challenging the current operating model

At a detailed level, firms are evaluating their current operating models across several key dimensions:

Structure

- **Location of resources.** Are the roles and responsibilities of each line appropriate, or do some roles need to be relocated closer to the origin of risk for faster and more effective detection and remediation?

- **Balance of resources.** Does the balance of resources—particularly between the first and second lines of defence—promote accountability and address fundamental needs at the origin of risk?

Alternative service delivery models

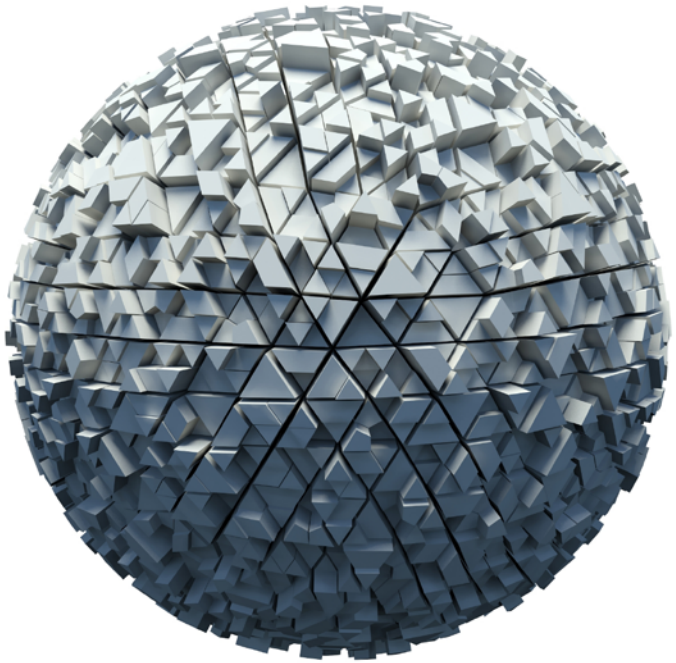
- **Centralization of key business processes.** How can key business processes be centralized on an enterprise level to be more efficient, effective, adaptable, and standardized? How can internal processes be controlled to increase quality across business operations, e.g., with centralized control testing and monitoring?

Three lines of defence

- **Capitalizing on subject matter experts (global centres of excellence).** How can subject matter experts for key areas—such as capital and resolution planning, vendor management, and cyber—be used to help inform both first- and second-line efforts in a manner that fosters consistency and quality?

- **Co-sourcing a portion of risk roles (managed risk services).** How might the use of third parties and/or offshoring produce better risk management at lower costs, particularly in areas where specialized talent is hard to recruit, or where repetitive tasks might enable an outside provider to achieve greater economies of scale?

- **Joint ventures (industry utilities).** How might joint ventures with other banking organizations enable costs to be shared across the industry for common activities, such as conducting annual due diligence for third-party vendors used by multiple banks?



Enabling operating models and controls rationalization and enhancements

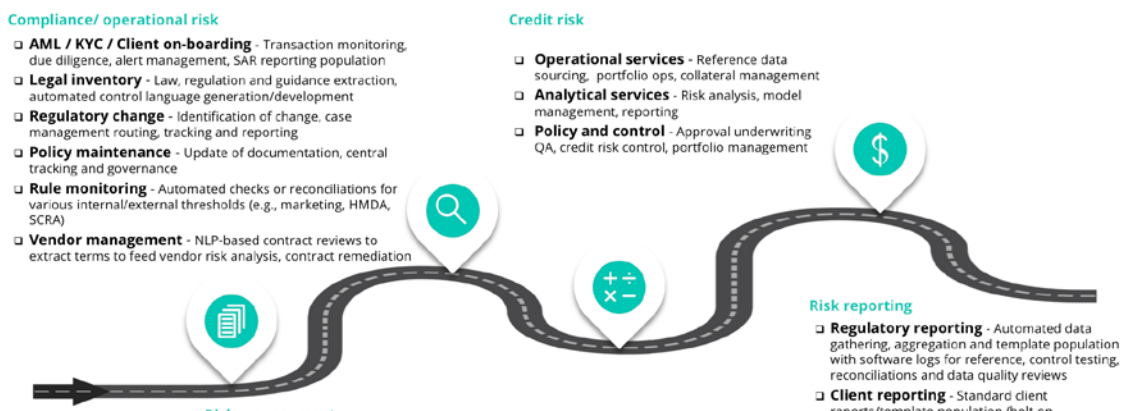
As part of the re-engineering process, firms should assess whether they have the right tools to enable transformation and allow their best and brightest employees to imagine and execute the art of the possible. Existing and emerging technologies can significantly aid in the transformation effort—helping to automate workflows, enhance platforms, generate advanced data analytics, and automate repetitive tasks.

Tools such as robotic process automation (RPA) and NLP can help firms eliminate essential but repetitive and mundane tasks, creating economies of scale and freeing up resources for higher value analysis. Advanced data analytics and reporting allow users to take advantage of the same data across the three lines of defence without creating redundancies, while at the same time enabling customizable views that fit the role and needs of each line.

When deciding how to move forward, firms need to consider whether investing time, energy, and money to optimize their three lines of defence model and capabilities—while raising costs in the short term—will be worth the future payoff of achieving better, more sustainable risk management performance at a lower cost. Of course, they also need to consider that the alternative might be making endless minor tweaks to inefficient systems that may or may not meet internal and regulatory expectations—and that may ultimately require a more expensive and distracting overhaul down the road.

Risk management of the future: areas of opportunity

There is broad applicability for these tools across risk and compliance domains. Below are some illustrative areas to consider:



Conduct

We continue to see global interest across jurisdictions in advancing a conduct and culture agenda. As a concept, conduct risk has taken on greater meaning since the financial crisis. Ten years ago, business practices and conduct started becoming more prominent topics. Five years ago, firms began establishing frameworks to identify, manage, and monitor conduct as a new dimension of risk. Today, numerous industries are coming to terms with how to proactively prevent employee misconduct and manage the related cultural implications.

However, progress to transform the governance and culture of financial services continues to be blighted by episodes of misconduct. As the root causes of misconduct are addressed, we expect authorities to bolster the supervision of firms' internal governance and controls, and focus increasingly on diversity as a bulwark against group-think. Appetite for enhanced accountability regimens is also growing. As we emerged from the global financial crisis, regulators highlighted the danger that firms become complacent about their governance and culture. Organizations will be expected to demonstrate that they take the issue of culture seriously and have in place governance and control frameworks that are resilient, stable, and robust enough to adapt to the current environment as well as identify new and emerging risks.

Firms will need to take particular care to ensure that their internal governance and control frameworks are adequately managing the risks, including to their customers and their operational resilience, which may arise from implementing innovation and technology. Supervisors, keen to preserve public trust, will expect firms' use of technology and innovation to be grounded by strong principles, including clarity of purpose, adequate oversight, and clear communication with customers.

Diversity can bring a broader range of skills and experience, and can also bring constructive challenge to the decision-making process. If firms are to avoid incidents concerning the misuse of personal data, a diverse and inclusive board may prove critical to ensuring that the technical and ethical implications of developments, such as increased use of AI or the use of customer data, are adequately considered and thought through.

FIs should also prepare themselves for a potential shift in regulatory focus toward greater accountability. They can begin by clarifying and documenting the roles and responsibilities of senior managers and other key individuals as well as communicating the expectations regarding accountability and conduct at all levels of the firm.

In Canada, the Financial Consumer Agency of Canada (FCAC) has culture and conduct issues as a top priority in its supervisory oversight. The year 2018 witnessed the introduction of a financial consumer protection framework in the Canadian government's latest budget implementation bill, signalling an interest in much greater standards of expectation for whistleblowing, complaints, and oversight of consumer protection issues by management and boards of regulated institutions.

Looking forward

Enterprise view of conduct risk

Large institutions are expected to have an enterprise-wide conduct risk management

Conduct

program and conduct risk function. The regulatory focus is on continuous monitoring of conduct and improvement, and detection and prevention mechanisms to influence how strategic objectives are being achieved.

The traditional focus on employee conduct is converging with a newer focus on market conduct, business practices, and impact on clients and markets. Also, there is significant focus on development of internal controls, creating a need to rationalize activities in order to efficiently manage the program. This may lead to some realignment of supervisory/surveillance activities.

Analytics and predictive intelligence applied to conduct and culture

Firms are also seeking to generate meaningful insight on employee conduct for the board, senior management, and regulators. The ability to predict and prevent employee misconduct is a business imperative across institutional, retail, and wealth management sectors. FIs want to identify employees with poor conduct sooner, proactively identify the next population of at-risk employees and activities, and develop improved approaches for heightened supervision and targeted surveillance/monitoring.

Challenges and opportunities from emerging technologies

Technology continues to disrupt how firms engage, deliver, monitor, and interact with customers. As a disruptor, technology gives rise to new business practices that can lead to new or increased conduct risks and challenges (e.g., digital banking, robo-advisors, electronic/algorithmic trading, and new products such as Bitcoin). However, it also creates opportunities to implement and refine controls that support sound conduct risk management (e.g., harnessing the increased availability of data to better predict—or more quickly detect—employee misconduct).

Compensation and remuneration focus

This continues to be a significant area of attention for regulators. The Financial Stability Board (FSB) is planning to release recommendations on how FIs can enhance their capacity to consider and monitor the effectiveness of compensation tools. The FSB's recommendations will also highlight mechanisms for promoting good conduct and addressing misconduct risk. In Australia, the Banking Royal Commission reviewed a number of financial services institutions and identified remuneration as one of the root causes of misconduct.

Key takeaways

As FIs revisit operating models in this era of technological innovation, cost reduction, business, and structural changes, they need to recognize that meeting regulatory expectations for safety and soundness can only be achieved by embedding governance, conduct, and culture.

Insights to action

- To maintain a resilient, adaptable and sustainable approach to risk and compliance, FIs should re-assess opportunities for innovation and productivity improvements in their risk operating model.
- Optimizing the risk and compliance functions may not only bring cost reduction and efficiencies, it also serves to **enhance scalability, agility and pace of response** to evolving business needs and future regulations and policies.
- Embedding a culture of awareness and reciprocal support will drive the optimization of the three lines of defence model. This culture can be achieved only if it's set by the tone at the top and matched by the tone in the middle.

Strengthening resilience

We are in an era of technological innovation, which has been a catalyst for FIs to re-examine operating models. As banking moves forward, risk management is subject to the same forces of innovation that the rest of the institution is facing.

This wave of innovation is challenging the convention of accepted and expected risk management practices. FIs are now looking to optimize their risk management approaches and systems to be more automated, more flexible, more capable of near real-time risk reporting, and more closely linked to firm strategy and risk appetite. While it used to be argued that the tenets of the three lines of defence were unassailable, FIs are now re-examining the model. Regulatory technology, or regtech, and the movement towards risk technology, or risktech, are becoming business imperatives.

In turn, the challenge to the financial services industry is how to innovate without weakening risk management. Managing risk innovation is top of mind for FIs and regulators alike. While regulators do not want to dictate to FIs how to manage innovation, they will challenge solutions if there is the potential for risk management to be compromised.

Looking forward

It is clear that business models are shifting. Factors such as access to financial services, open banking, fintechs, and technological innovation along with the regulatory landscape will continue to evolve and to force change. It is no longer a question of whether these things will unfold and transform the industry—it is already happening. FIs that proactively embrace innovation rather than treat it with arm's-length skepticism and that foster a culture of conduct and strong governance will strengthen their resilience to forces in the marketplace and be at a clear advantage.

Glossary

AI - Artificial Intelligence
AML - Anti Money-Laundering
BCBS - Basel Committee on Banking Supervision
CARR - Canadian Alternative Reference Rate Committee
CDO - Chief Data Officer
CDEs - Critical Data Elements
CORRA - Canadian Overnight Repo Rate Average
CRR2 - Capital Requirements Regulation II
CRR3 - Capital Requirements Regulation III
EBA - European Banking Authority
EU - European Union
FCA - Financial Conduct Authority
FRTB - Fundamental Review of the Trading Book
FIs - Financial Institutions
FSB - Financial Stability Board
IBOR - Interbank Offered Rate
IMA - Internal Models Approach
IT - Information Technology
LIBOR - London Interbank Offered Rate
ML - Machine Learning
NLP - Natural Language Processing
NMRF - Non Modellable Risk Factor
OSFI - Office of the Superintendent of Financial Institutions
P&L - Profit and Loss
QIS - Quantitative Investment Strategy
RWA - Risk Weighted Asset
RFRs - Risk Free Rates
RTR - Real Time Rail
SA - Standardized Approach

Endnotes

1. Institute of International Finance, *Global debt monitor*, July 2018.
2. International Monetary Fund, *Bringing down high debt*, April 2018.
3. Alex J Pollock, *Financial crises occur about once every decade,* Financial Times, March 2015.
4. E*TRADE Capital Management LLC, *Where are we in the current business cycle?,* June 2018.
5. European Banking Authority, *Risk Dashboard Data*, Q2 2018.
6. Financial Conduct Authority, *Transforming culture in financial services*, March 2018.
7. Deloitte, *Economic outlook: Singing the late-cycle blues*, https://www2.deloitte.com/ca/en/pages/finance/articles/economic-outlook-singing-late cycle-blues.html, accessed December 3, 2018.
8. Financial Conduct Authority, *The future of LIBOR*, https://www.fca.org.uk/news/speeches/the-future-of-libor, July 2017.
9. Deloitte, "*Fintech by the numbers: Incumbents, start-ups, investors adapt to maturing ecosystem*", 2017.
10. ACI Worldwide, Universal Payments, "*Immediate need for fraud prevention,*" 2016, https://www.pymnts.com/wp-content/uploads/2016/09/Best practices-for-preventing-fraud-in-a-real-time-world.pdf, accessed April 26, 2018.

Contacts

Michael Chau
Partner, Risk Advisory
416-601-6722
michau@deloitte.ca

Azer Hann
Partner, Risk Advisory
416-601-5777
ahann@deloitte.ca

Jay F. McMahan
Partner, Risk Advisory
416-874-3270
jfmcmahan@deloitte.ca

Bruno Melo
Partner, Risk Advisory
416-601-5926
brmelo@deloitte.ca

Mariama Zhouri
Senior Manager, Risk Advisory
514-393-7317
mzhouri@deloitte.ca

We wish to thank the following Deloitte client service professionals for their insights and contributions to this report:

Jas Anand, Senior Manager, Risk Advisory, Deloitte Canada
Andrea Barragan-Verduzco, Senior Consultant, Risk Advisory, Deloitte Canada
Olivia Chiu, Senior Manager, Risk Advisory, Deloitte Canada
Sandeep Chopra, Senior Manager, Risk Advisory, Deloitte Canada
Robert Cranmer, Director, Risk Advisory, Deloitte Canada
Judit Halin, Partner, Risk Advisory, Deloitte Canada
Umang Handa, Senior Manager, Risk Advisory, Deloitte Canada
Stefanie Ruys, Senior Manager, Risk Advisory, Deloitte Canada
Betty Tien, Senior Manager, Risk Advisory, Deloitte Canada
Slava Trefilin, Senior Consultant, Risk Advisory, Deloitte Canada
Helen Zhang, Manager, Risk Advisory, Deloitte Canada
Zeshan Choudhry, Partner, Risk Advisory, Deloitte UK
Scott Martin, Senior Manager, EMEA Centre for Regulatory Strategy, Deloitte UK
David Strachan, Head of EMEA Centre for Regulatory Strategy, Deloitte UK
Pierre Lapointe, Partner Risk Advisory, Deloitte Canada
Jacques Guvlekjian, Senior Consultant, Risk Advisory, Deloitte Canada

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on **LinkedIn, Twitter** or **Facebook**.

Deloitte.