Deloitte.

Innovation in risk management

Canadian regulatory outlook for financial institutions in 2018

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Contents

Foreword

Uncertainty unclarified

Another year has passed, so what has changed?

This time last year we expected 2017 to be a period of uncertainty for financial services regulation. Financial services firms were challenged by the continuing lack of clarity over the final shape of post-crisis reforms, the implications of Brexit, and a new US political administration. We also saw significant pressures on the banking and life insurance sectors from sluggish economic growth and low interest rates in Europe and the US, and competition from new entrants (particularly fintechs).

Looking ahead to 2018, most of these challenges and uncertainties remain.

Economic growth, but how robust?

Global growth prospects improved through 2017 and continue to be broadly positive, albeit more subdued than in the period before the financial crisis. China, Europe, and Japan have all been outperforming expectations, and although India's economy has slowed lately, the long-term outlook is upbeat. There are now signs that the extraordinary monetary easing of the last 10 years is starting, slowly, to unwind in Europe and the US, although this stands in contrast to the situation in China and Japan.

There are reasons for caution. Asset markets and prices have seemed impervious to the prospect of tighter monetary conditions and geopolitical tensions. This has left many commentators worrying that markets are in the grip of a bout of irrational exuberance. There are also signs of price bubbles in commercial and residential property markets, leveraged finance markets, and elevated levels of consumer indebtedness, particularly in the advanced economies.

Supervisors across the globe are very alert to the financial stability risks posed by the political and economic climate, and we expect them to focus on the ability of financial institutions in all sectors to deal with the downside risks of an abrupt shift in market sentiment and any increase in asset price volatility, irrespective of the trigger. Boards are expected to keep their risk appetites under review. They will also need to engage closely with stress testing, whether prompted by supervisors or carried out internally.

What does this mean for the regulatory agenda?

Last year we predicted that there would be no wholesale rolling back of the post-crisis regulatory framework, and this remains our view. The consensus in the US is that there will be some meaningful adjustments to the Dodd-Frank Act, but no large-scale repeal or re-write. In the EU there remains a considerable volume of legislative work ongoing; and even where there is no new legislation, there is a great deal of "fine tuning" of existing rules. The Asia Pacific region faces a long tail of implementation work, and must also deal with the impact of regulation from outside the region.

At the international level, the Financial Stability Board (FSB) has shifted its primary focus towards a post-implementation evaluation framework, which will be "progressively applied" in the coming years.[1] This is part of a rebalancing away from introducing new rules toward assessing the effectiveness of what has been done over the past decade. Boards will need to be ready to demonstrate to supervisors that they have embedded change and that this is leading to the desired outcomes.

One major area in which there remains a number of significant unanswered questions is bank capital requirements. Although the Basel Committee on Banking Supervision (BCBS) has until now been unable to complete the Basel III package, final agreement on the open issues seems within reach. We do not see any major economies as being in a hurry to introduce yet more legislation, and we also see those economies being more willing to depart from the letter of global standards where they conclude it is in their interest to do so.

As a consequence, financial services firms need to be prepared to deal with the challenges of diverging regulatory frameworks. At a minimum they will need globally coordinated approaches to understand overlaps, incompatibilities, and potential synergies.[2]

Supervisors are turning more attention to long-term structural issues

Technological innovation, aging populations, and climate change have all caught the attention of the regulatory and supervisory community as emerging risk areas. We expect some supervisors to begin to challenge boards, risk committees, and senior management to demonstrate that they understand the impact on their customer bases, business models, and risk profiles, and are set to take effective mitigating actions where needed.

---

[1] See FSB, "Implementation and Effects of the G20 Financial Regulatory Reforms", 3 July 2017
[2] For more on a divergence resilient approach see the Deloitte report "Dealing with divergence: a strategic response to growing complexity in global banking rules"

Fintech:

While new technologies present opportunities, regulators want to understand the potential risks and the likely impact on incumbents' business models. The FSB has a clear interest in the subject. The European Commission is expected to deliver a fintech "Action Plan" in January. Similarly, US regulators are considering the implications of new technologies, including third-party relationships among fintechs and banks, and are even exploring special purpose bank charters for fintechs.

Climate change:

The FSB has taken the lead internationally with its Task Force on Climate-Related Financial Disclosures, which made its final recommendations in June 2017. A number of regulators in the Asia Pacific region are instituting policies to encourage green finance. The BoE is also researching climate change and the EU recently proposed to integrate environmental risks into the mandates of the ESAs as part of its Action Plan on sustainable and green finance.

Aging populations:

Aging populations worldwide will create a widening pool of potentially vulnerable customers and influence demand for different types of financial services, as well as the way in which financial institutions engage with their customers. At the international level, the International Organization of Securities Commissions is taking forward work on aging populations.

Leadership changes

Lastly, we note that by the end of 2018, the most senior leadership of many of the world's most important regulatory bodies will be starkly different from what it has been for the majority of the post-crisis regulatory reform era. Mark Carney's term as chair of the FSB has been extended through to December 2018, lending some additional continuity to reform efforts, but this will be his final year at the top of the FSB. We expect Stefan Ingves to stand down as chair of the BCBS in the near future. There is also a great deal of change in senior leadership across national and regional regulatory bodies, particularly in the US. It remains to be seen how far new leaders will uphold the key tenets of the international supervisory agenda of the last decade, particularly its emphasis on cross-border coordination, or whether supervisory priorities will tilt more towards promoting the competitiveness of individual jurisdictions.

On balance we think these new leaders will emphasize practical supervisory initiatives over (new) rule-making, as well as the need for firms to demonstrate that they are financially and operationally resilient to a range of threats, both old and new. New leaders will be keen to consolidate the outcomes and achievements of the prudential policy agenda that has dominated the last 10 years and focus their tenures on continuing structural challenges as well as emerging risks and issues.

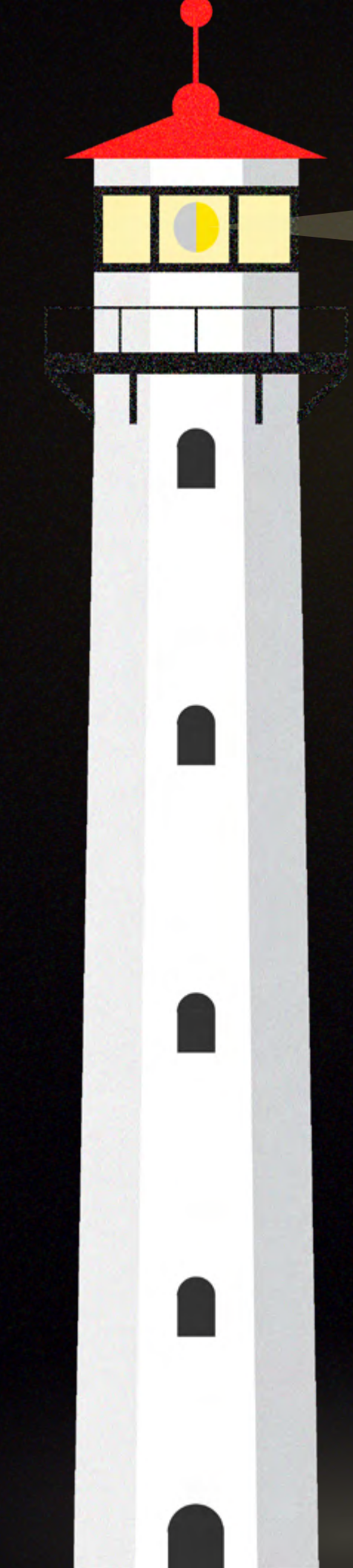
Acting in the face of uncertainty

While we expect some greater clarity about the regulatory outlook to emerge in 2018, the overriding challenge for firms remains coping with uncertainty, including from the global impacts of Brexit and how markets in Europe and elsewhere will be reshaped by the Markets in Financial Instruments Directive (MiFID) II. This will put a premium on firms maintaining strategic flexibility, while at the same time adopting new technologies to react to the threat from "challengers", improve their customer service and outcomes, better manage their risks, and help control costs. With yields and income levels, and therefore return on capital, still under pressure, cost control will continue to be important: even though interest rate rises are underway, they will be neither quick enough nor big enough to alleviate pressure on incumbents' business models.

Kevin Nixon
Center for Regulatory Strategy
APAC

Chris Spoth
Center for Regulatory Strategy
Americas

David Strachan
Center for Regulatory Strategy
EMEA



Introduction

Now a decade past the transformative events of the 2008 financial crisis, we have a better perspective on the evolving nature of its impacts.

When we consider how financial institutions (FIs) approached risk management a decade ago, it makes sense that the industry's initial reaction was to strengthen the oversight and control functions related to risk management, in all their many organizational shapes and sizes.

At the start of 2018, we have reached a point at which competitive pressures on the financial services industry are driving a shift in approach, making this an opportune time to rethink how all the control functions—risk management, compliance, finance, and internal audit, among others—can deliver more strategically on their mandates. Indeed, these pressures are driving FIs to search for stronger efficiencies (through better collaboration across the control functions) and enhanced effectiveness (to stay in front of new and emerging risks).

With this imperative in mind, leading organizations are broadening options, embracing innovation in the regulatory and risk management domains in real ways, including the underlying operating model. Some FIs, for example, have begun to question the fundamental role of risk management, wondering if certain aspects of the "three lines of defence" concept needs to be rethought. The recent growth of control functions may have helped with the optics of stronger oversight and risk management, but it has arguably not been as effective as was first hoped. Now, second-line functions are looking to become more focused and efficient, with the first line (business units) assuming a bigger risk management role.

Along with this control model shift, the competition from tech- and analytics-driven startups and financial technology firms (fintechs) is pushing FIs to explore how to benefit from new capabilities in areas ranging from credit adjudication to monitoring external cyber threats. The growing emphasis on digital channels and enhanced customer experience is also placing pressure on firms to consider innovative solutions.

Together, these trends will also affect organizational approaches to talent management. The necessity for new operating models and enhanced productivity from controls means that the diversity of capabilities will need to broaden. This is vital not just for how the control functions operate their own mandates but also how they can improve their interactions with business partners in pursuit of innovative digital and mobile products and services. In future, control functions will capitalize on an increasingly diverse talent pool—including people steeped in advanced analytics, artificial intelligence, and automation—to remain relevant and valuable to their business franchise.

Bearing these potentially transformative shifts in mind, I'm pleased to introduce *Innovation in risk management: Canadian regulatory outlook for financial institutions in 2018*. This overview offers key information and insights on some of the most critical regulatory topics for 2018, examining how trends such as innovation, automation, and analytics are becoming increasingly imperative when addressing regulatory priorities and competitive demands.

Jay F. McMahan
National Leader
Deloitte Centre for Regulatory Strategy
Deloitte Canada

Financial risk

While financial risk management is important in all industries and sectors, it has always been, and remains, particularly critical for financial institutions (FIs).

Today's rapidly changing global environment demands both financial stability and liquidity, which means the continuous application of rigorous governance, robust processes, and accurate models across the finance function.

At the same time, the financial services industry is itself in a period of heightened change and uncertainty. As the competitive landscape evolves—with rising competition among FIs and fintechs driving growth and innovation—the FI ecosystem is redefining what the future of financial services will look like, developing new retail products, alternative investment vehicles, and volume-centric sales and marketing strategies.

This creates a quandary. While failing to innovate may put FIs at a competitive disadvantage, doing so without aligning business strategies with sound risk management practices may heighten both strategic and financial risks. As a result, FIs that develop risk management frameworks that are both strong and innovative—ones that satisfy compliance demands, while enhancing decision-making and driving performance—will have a clear competitive advantage.

As these trends continue apace, three critical areas FIs are looking to focus on in 2018 are: fundamental review of trading book (FRTB), International Financial Reporting Standard 17 (IFRS 17), and model risk management.

Fundamental review of trading book

Scheduled to become effective in early 2022, FRTB is a globally applicable standard for measuring market risk in FI trading portfolios. It's one of the biggest changes to this risk area in many years: at a minimum, FIs must comply with the Standardized Approach (SA) to retain their ability to transact in products as defined by the new regulation. This means the entire organization is affected, not just the trading businesses.

The capital requirements as defined by the SA calculation have been introduced to allow regulators to perform comparisons across FIs. Trading book capital as calculated by the advanced method (also known as IMA) includes the expected shortfall (ES), prompted by the significant shortfalls seen in trading book capital during the financial crisis. ES asks the question: "if things do go badly, what is our expected loss?" whereas Value at Risk (VAR) asked: "how bad can things get?"–ES considers the average of all losses that are greater or equal than the VaR. The IMA replaces the VaR calculation and generally results in a higher, more risk-sensitive capital requirement. FRTB also has stricter disclosure requirements and validation standards.

The most obvious impact of this enhanced standard will be that trading book capital requirements will increase. The amount of the increase will depend on the compliance approach an FI chooses. Under SA, capital could go up by as much as 400 percent while under IMA, it might increase by 15 to 40 percent. On a blended basis (as some portfolio holdings cannot use IMA or get no benefit from it), the market risk capital required will still significantly increase over current levels.

Since market risk capital can currently represent on average 15-20 percent of the total risk capital a bank needs to hold, the impact of FRTB is clear. On the plus side, there will be a number of potentially less obvious benefits: for example, profit and loss (P&L) calculations, currently performed separately and often yielding different results, will have to be much more aligned under FRTB. Achieving compliance will provide the opportunity to review the broader operational landscape of the business and the platform from which to effect related, non-FRTB changes. Strategic decisions concerning other areas—such as products, geographies, and client interaction models—could also be in scope for review.

FRTB and innovation

Given how broadly FRTB's requirements cut across financial calculation, performance measurement, trading desk structure, and more, banks will have to apply more rigour to the long-standing issue of data management and data consistency. This should be viewed as a strategic business opportunity rather than a compliance obligation. Implementing FRTB's new profit and loss attribution (PLA) test will require FIs to more closely integrate their risk and finance divisions—indeed, the entire organization—to better share and manage transaction data. This will require an assessment of data, process, and technology architectures, to understand any upgrade needs to meet FRTB requirements. Manual processes will be inadequate, and many major banks are well into in multi-year upgrade initiatives in this area.

From insight to action: preparing for FRTB

To get your organization ready to meet FRTB, consider taking the following steps:

- **Complete** the Basel-requested quantitative impact study (QIS) to determine the capital impact and identify areas for deeper analysis.
- **Align** information aggregation structures, particularly between finance and risk.
- **Ensure** financial products are identified with a common taxonomy so they are recognized as the same product across the organization; by applying the same definitions, disparities are eliminated and consistency achieved.
- **Enter** into industry-wide collaborations to share pooled information so all entities have the required number of observable prices relative to a particular risk factor.
- **Ensure** decomposition capabilities; that is, the capability to calculate risk on each constituent stock within any traded index. If this isn't available, capital holding requirements will increase.

Get a jump on talent acquisition

Canada's major banks are at different stages of FRTB preparation and maturity. Those that are lagging will have greater difficulty securing strong capabilities and experience as time passes. One aspect of critical planning for the initiative is not seeing it as a risk-only initiative or as a regulatory requirement for only the risk function to solve. FRTB programs and solutions should be co-sponsored by the front office and risk, to ensure the right sponsorship, oversight, and strategic focus.

Canadian FIs also need to act now to ensure they have the right talent required to implement the technological requirements of FRTB. Europe, the UK, Asia, Australia, and South Africa all began FRTB preparation before most Canadian FIs, so we have a lot of work to do to develop—or import—the right people, capabilities, and resources.

FIs should take advantage of the relatively long FRTB implementation timeframe to review larger aspects of the business as the impact of changes become evident.

By looking closely at loss leaders or marginal business areas that could be exited, it could also be an optimal time to restructure.

International Financial Reporting Standard 17 (IFRS 17)

IFRS 17 is an accounting requirement specific to insurance companies. Designed to improve the comparability of financial statements, it will replace local Generally Accepted Accounting Principles (GAAP) with one single model for measuring insurance contracts for both life and property and casualty (P&C) insurers.

The standard will affect multi-year contracts and how both life and P&C insurance companies report on those contracts in their financial statements. It's a complex standard that will be challenging and time-consuming to put into practice, and takes effect January 1, 2021. For insurers, the transition to IFRS 17 will have an impact on financial statements and on key performance indicators. This ultimately results in impacts on an organization's IT system, strategic management, and employee skillsets as well as business processes. This is an opportunity for organizations to re-evaluate their business model as well as make changes to their financial reporting infrastructure.

Upon initial review, IFRS 17 may appear to be more relevant to accounting. However, the risk function must be closely involved in its implementation because of the challenges associated with overhauling major systems and data technologies, which will be a major compliance requirement. It will affect processes across the organization, including accounting, reporting, controls, planning, actuarial, product design, pricing, risk management, and certain operational processes, all of which affect the financial statements. Indeed, some companies will need to design and implement entirely new core processes to reflect new contract models and calculations, which in turn will then require new controls and procedures for contract valuation and disclosure. They must also ensure the right data is available within those systems to drive consistency and accuracy for the financial statements as well as to measure key performance indicators.

The risk domain implications resulting from such changes are numerous. What might this level of transformation mean from a capital and financial reporting perspective? Are models being specified appropriately? How is information being tracked and stored? How is accuracy being tested? How are the people who have the right knowledge and capabilities to execute this mandate being acquired and retained?

As insurers work to answer these questions, they should prepare for a number of significant, specific impacts. For example, IFRS 17 will affect both balance sheet and income statement processes as well as increase the volume and complexity of disclosures around amounts, judgments, and risk. In some cases, there will be variances between the two types of insurers; for example, extensive impacts on multi-year contracts will be most felt by life insurance companies, though some P&C commercial contracts will be affected. Operational challenges regarding processes, systems, and data will also be greater for life than P&C insurers. Both, however, will have to deal with much higher actuarial data volumes and modelling changes. All these changes ultimately require awareness and readiness of the organization to deal with the business and financial impacts.

Firms cannot lose sight of the fact that IFRS 17 is more than an accounting issue. Stakeholders in HR, IT, communications, and product strategy will all be affected—and risk must be addressed in all those areas.

IFRS 17—where does innovation fit in?

Major IFRS 17 changes will require new tools and technologies to be implemented, so organizations could use those advances to generate new efficiencies, redesign processes, and improve the organization beyond the regulatory mandate minimums. Since insurers are being compelled to look at their processes and evaluate how those processes will need to change, insurers could take the opportunity to redesign on a larger scale and see what other automated, systematized processes could be incorporated.

From insight to action: toward IFRS 17 implementation

To prepare, consider taking the following steps:

- **Develop** a clear roadmap, detailing the IFRS 17 journey as far as you can. Add to it as strategy unfolds and more information becomes available.
- **Undertake** a business impact assessment: document current processes, identify gaps in both processes and systems architecture, and determine what must be done to close them.
- **Undertake** a financial impact assessment to quantify these impacts. What key products are affected, and how can the results be consolidated and reflected on the balance sheet?
- **Implement** organization-wide training and education so your people understand what's going to happen. Make sure to cover planning and forecasting, changing roles, risk management teaming, product development, pricing, finance, and tax.

Model risk

The risk of incurring losses caused by flawed quantitative financial models has long been a concern for FIs. The focus on robust model risk management has increased after the solvency and liquidity events in the financial crisis of 2008, which clearly highlighted the risk of unexpected loss due to incorrect valuations.

Having become more concerned about systemic model risk in general, global regulators have begun introducing more stringent model risk management requirements. The issue is now particularly germane in Canada following the publication of Guideline E-23 for model risk management in September 2017 by the Office of the Superintendent of Financial Institutions (OSFI). OSFI's formal guidance expands on frameworks such as that published by the Federal Reserve and the Office of the Comptroller of the Currency in 2011 in the US, the Supervisory *Guidance on Model Risk Management* (SR 11-07).

Additionally, OSFI has decided that standardized institutions, as defined in the guideline, will have until January 1, 2019, to become compliant with this guideline. The remaining institutions (i.e. internal models approved institutions) are expected to comply with the guideline by November 1, 2017.

Balancing technological reliance is an innovation in itself

The modelling domain has traditionally been the province of quantitative specialists and technical designers. However, today the focus of innovation is moving away from relying on highly complex models as a singular panacea, but instead conceding that models are limited in their ability to describe and simulate the world.

What is needed instead—or in addition—is on-the-ground governance of the business, including the models used to run it. This requires boards and management to ask questions, such as:

- For what specific purpose are models being used?
- What could happen if the wrong model or the wrong parameters are used?
- What if those charged with using a model are not using it properly, or are using it fraudulently?
- What level of trust and confidence should leaders have in the models they use?

From insight to action: How FIs can facilitate model risk compliance

Consider taking the following steps:

- If you are a subsidiary banking operation, **don't assume** that you can fully rely on a parent company's model risk controls. Branches may have important obligations to ensure their own compliance.
- **Take** an inventory of model usage, materiality, and complexity within the organization to identify where risk gaps may exist.
- **Make sure** the models you use are appropriate to the firm's size and needs.
- **Undertake** or commission a specific E-23 gap analysis to identify specific impact areas, who will be affected, and if you need to establish new risk practice areas, such as a model validation function.
- **Ensure** an appropriate level of senior involvement in modelling throughout the firm. Any assessments must be communicated fully to senior decision-makers, clarifying any potential exposures.
- **Ensure** data transparency, model reliability and applicability, and ongoing model improvements all support more effective decision-making, adding genuine organizational value.

Model risk management requires an integrated platform

It's important for regulated FIs to focus on E-23 compliance in the short term. However, as model risk management technology capabilities becomes more sophisticated and model governance comes under greater scrutiny, Canadian FIs should look to establish a more holistic, customized model risk management framework—one that can effectively deal with the increasing complexity of models and their application.

Regtech

A combination of high-profile oversight and compliance failures along with a growing sense of eroding public trust in institutions broadly suggests that the volume of regulatory requirements and rising expectations for compliance will not diminish in the near term.

Policymakers, regulators, and shareholders are looking for firms to not only meet new regulatory requirements but also to ensure a robust program of continued compliance. As a result, the operating costs for compliance and risk mitigation will continue to rise in the near term for retail and corporate banks.

However, innovative organizations are now challenging the orthodoxy of the cost of compliance and experimenting with new capabilities–often technology-enabled. As a shorthand for regulatory technology, regtech is now moving to the centre of efforts to tackle this productivity challenge for regulatory compliance demands. Many regtech innovations offer significant transformative potential and operational improvements. Indeed, regulators are generally encouraging firms to develop environments that use these technologies, though many organizations are struggling to do so in the most efficient manner.

While automation initiatives may reduce process risks by eliminating manual tasks and automating certain controls to improve efficiency and effectiveness, they also introduce new operational, regulatory, financial, organizational, and technical risks, all of which must be mitigated.

Robotic process automation, machine learning, and blockchain are three dimensions of regtech innovation that FIs are starting to adopt to help meet these objectives.

Robotic process automation

Robotic process automation (RPA) is one of the increasingly common regtech options that is being used to automate repetitive tasks. It has been characterized as "spreadsheet macros on steroids", with the critical difference being that RPA tools allow the automation of repetitive actions across systems, including websites, email, and folder structures.

In a financial institution, high-volume repetitive tasks can occur in several business processes, whether it is entering data into a system, reading it from a document, or transferring data between an external system and internal systems. For instance, investigations require a large number of highly repetitive tasks: consider that if 150 investigators are handling an average of two cases each per day, a large percentage of this labour is directed toward manual administrative and repetitive tasks that could be re-directed toward more productive investigative work.

This is where RPA can demonstrate its greatest value, by reducing the manual efforts to aggregate data from multiple sources while increasing the quality of compliance monitoring and testing. Deployment in this instance enables FIs to optimize their compliance-reporting processes by centralizing aggregation and reporting abilities. RPA helps companies attain efficiency in executing such tasks, ultimately reducing costs.

An active engine of innovation

Technology alone doesn't deliver innovation: it also needs to be applied in innovative ways. Organizations should integrate RPA into their existing compliance environment in ways that make sense and deliver value. They need to know how to deploy it and understand both the inputs it requires and the outputs it promises to deliver.

In theory, one technology could potentially deliver different innovations across multiple organizations. The most important impact of RPA, though, may be its ability to make compliance a leaner function, while remaining an effective one that becomes more scalable, less expensive, and better able to focus on its more challenging, non-repetitive duties.

From insight to action: putting RPA to work

Taking the following steps may help move you toward implementing robotic process automation:

- **Develop** a regtech strategy that defines how and where RPA will be deployed in the organization. Consider areas in which there are many highly manual processes involving multiple systems, as these will be most ripe for productivity improvement.
- **Ensure** you have diverse talent in place combining a deep understanding of regulatory requirements, extensive experience with existing enterprise compliance processes, and robust knowledge of the RPA solution and its effective application.
- **Develop** a sensing approach to analyze regtech vendors and emerging technology capabilities ecosystem.
- **Recognize** that RPA implementation isn't just a technology project. To be effective, it needs to be fully embedded in and integrated with your overall compliance program.

Canada: slower off the mark with RPA

The financial services industry in the United Kingdom is currently ahead of Canada in the adoption of RPA capabilities. US companies appear to be embracing RPA more proactively than Canadian ones, with more proof-of-concept projects underway overall. Canadian firms are considering ideal use cases for RPA. Several of them have gone through proof-of-concept implementations and are in the process of scaling.

Machine learning

In a broad sense, machine learning describes a form of artificial intelligence (AI) in which a machine or system is able, without explicit programming, to interpret information, determine the next action, then continue to determine actions based on both additional input and previous results. The system reacts to given input, essentially picking up patterns and learning on its own, within certain boundaries.

Notably, such machines don't have to be pre-programmed for each individual pattern they're designed to monitor. Over time, they will begin to identify them on their own. Machine learning examples in day-to-day life include product recommendations that appear when we browse, email spam filtering, and credit-card fraud monitoring.

The promise of this technology is enormous. It enables us to create an intelligent, robotic workforce. While RPA is part of that equation, it can still create a bottleneck that requires human intervention. Machine learning takes automation to the next level by understanding two steps ahead and providing next-step options to the user.

For example, machine-learning engines like Intelligent Document Extraction and Analysis (IDEA) quickly identifies and extracts key terms from the document review process, which frees up time for analysts to perform value-add analysis. And the text-mining capability provides real-time analysis of data extractions to quickly diagnose missing information.

The impact of machine learning will be broad and significant. It will allow organizations to more efficiently monitor transactions for fraudulent behaviour, monitor the trade desk to ensure compliance with rules, handle trade surveillance, monitor staff behaviour, detect cyber abnormalities and intrusions, and track money-laundering activities. Before these opportunities can be realized, however, FIs must consider how to deploy this technology to help solve a business need or problem, as well as how to monitor and control these algorithms once they're put into use.

The latter issue poses new risks. If a machine is learning and operating itself, how does the organization know it's thinking intelligently? How can the machine be validated to ensure it hasn't taken a wrong turn in its thinking? How are the algorithms used being vetted and their performance over time monitored to ensure they continue to perform as expected and that unforeseen errors aren't growing?

If the algorithms begin to provide inaccurate information over time, it could have highly adverse effects on business performance, reputation, and more. These are important questions that must be addressed as machine learning is integrated further into business and compliance processes.

Speeding the pace of innovation with machine learning

We outlined at left a number of tasks that machine learning is already poised to enable. The future of machine learning holds even more promise, such as eliminating human-caused bottlenecks in the decision-making process. Rather than having risk managers do a manual comparison between regulatory mandates and existing control structures, for example, machines could be used to interpret new regulations and identify potential compliance gaps. Admittedly, machine learning would have to be complemented by human cognitive capabilities to accomplish this, but this is the sort of top-tier innovation we expect to see in future.

From insight to action: how do we seize machine-learning opportunities?

To lay the groundwork for this transformative technology, consider taking the following actions:

- **Identify** opportunities where machine learning can provide a real benefit. Start by identifying your pain points—the regulations that cause you the most challenges—and then evaluating where machine learning can help.
- Once an opportunity is identified, **pick** a subset and run a proof of concept to determine how it fits into your overall strategy and what risks it may introduce.
- **Focus** on a governance structure with the engagement of relevant members of the executive management to help manage risks and maximize value. Who will be responsible for first, second, and third line of defence reviews? Who will validate the model was created properly? Who will evaluate that it remains valid over time?

Canada's stance on machine learning

Regulatory requirements about implementing machine learning exist in Canada, but they're focused on the international community and are not FI-specific. Given the uniqueness of Canadian privacy laws, organizations should also consider how the implementation of machine learning might affect compliance in that area.

Blockchain

Blockchain is a distributed ledger or database that records digital interactions in a way that's designed to be secure, transparent, immutable, and auditable without having to rely on a trusted intermediary. It's a truly disruptive technology, with its ability to embed trust and integrity into business processes—a capacity that can help solve complex risk issues in new and novel ways.

For financial institutions, blockchain is most commonly applied to digital identity, trade finance, and international money transfer use cases. With trade finance, it maintains a copy of the ledger so funds can be cleared and settled between entities with increased transparency, security, and immutability.

As a technology, blockchain is evolving rapidly. The financial services industry has moved from proof of concepts and pilots to live implementations. We've already seen this innovation move from experimentation through exploration, then on to full integration with organizational ecosystems where it can facilitate real-time, productive transactions. FIs are now even starting to take advantage of blockchain for cross-border payment and currency exchange solutions.

Blockchain can also be used to gain competitive advantage. Recently, Deloitte helped a leading financial institution decide whether to capitalize on its blockchain implementation to service regulatory reporting requirements. We were involved in testing the ability of a platform to provide individual nodes to allow fund administrators to store and analyze fund data while coding regulatory reporting requirements into smart contracts for execution and data validation. A regulator node was also created, allowing the safe and secure exchange of data between firms and the regulator.

The main disruptive factor is that we are moving from a central authority being responsible for settlement toward an automated capability to transact with non-trusted parties on a very low-risk basis. Many FIs are currently in the exploration stage of adopting blockchain functionality, choosing instead to proceed slowly, carefully consider risks, deepen knowledge, and only add known or trusted parties to their ecosystem—this marks the biggest difference between FI applications and what other innovators are doing. In fact, FIs have regulatory obligations to only transact with trusted parties, so it's a challenge to make full use of blockchain capabilities while still remaining compliant.

A double-edged sword for risk

Blockchain is playing a crucial role in solving some of FIs' key risk issues, such as central clearing and settlement systems. These are very risky because they're slower than most other clearing systems, all their information is stored in a central location, and they're heavily relied upon. Distributed general ledgers reduce some of these risks, but as with all innovations, new capabilities and functionality can introduce new and possibly unanticipated risks. And criminals will inevitably find new and different ways to exploit blockchain technology.

With that in mind, organizations must perform risk assessments at the right time—prior to launching a pilot and while in production—to be confident they're doing their best to identify risks and implement proper mitigating controls. Although blockchain can help improve risk management, its potential to introduce new risks may keep regulators from accepting it as a compliance solution.

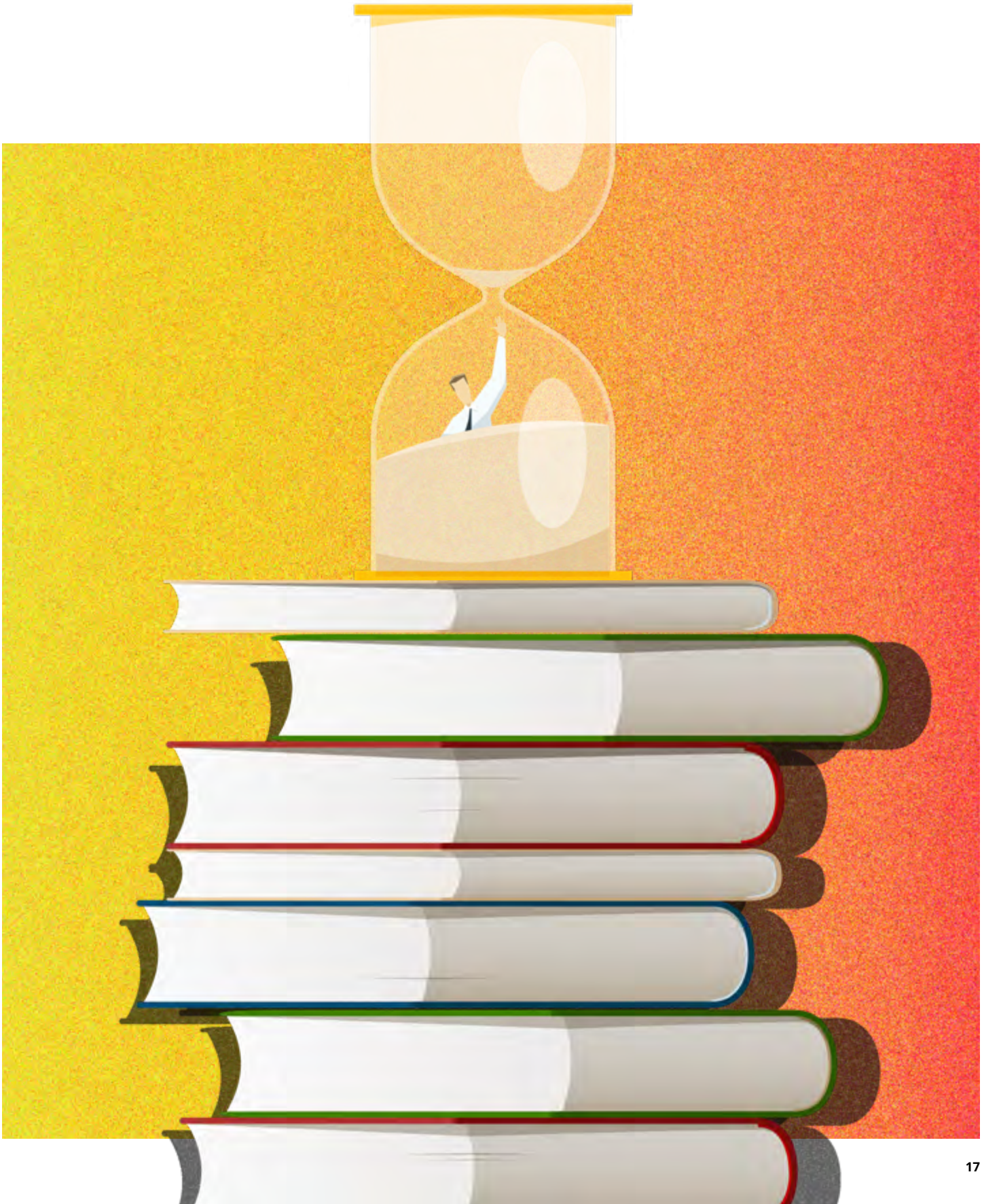
From insight to action: how FIs can best use blockchain capabilities

Start by exploring how blockchain may fit into your organization:

- **Try** to understand the minimum viable ecosystem in which a distributed ledger technology should operate. It's only a differentiator when multiple parties share the information and participate in the blockchain, so FIs must ask: who do I want to include in this system?
- **Determine** whether blockchain technology provides enough of a difference compared to traditional technology for the use case you've selected. Ensure the features available on a specific ledger provide differentiated solutions or offerings that you really need.
- **Launch** a live production pilot. Start with a smaller ecosystem then expand the number of participating parties until you've covered everyone in that particular value chain.
- **Develop** a cyber strategy to ensure you have appropriate key management rights and the right encryption to manage and store the keys.
- **Adopt** a Distributed Ledger Technology (DLT) risk management framework, to evaluate proposed pilot benefits and results relative to a broader enterprise risk environment -assessing the organization's control strength for inherit and residual risks.

Is Canada leading or following?

When it comes to regulating technologies, Canadian regulators tend not to be first out of the gate. They usually follow other countries such as the US or UK, or perhaps China. That said, blockchain is one instance in which Canadian FIs are leading the way on implementation. This is an advanced capability relative to other global regions because it involves such a large consortium of organizations. Canada is generally considered to have one of the most successful blockchain implementations in the world.



Culture, conduct, and compliance

Culture, conduct, and compliance represent three inter related dimensions that intersect to create fair outcomes for customers and help protect market integrity.

They also represent areas of intense scrutiny, as FIs in particular respond to the perceptible decline in customer trust that institutions of all kinds are experiencing. Much of this decline is due to the wave in recent years of high-profile wrongdoing that resulted in public regulatory censure and punishment. An impression of misbehaviour and of consumers being mistreated lingers with the public. It's a global phenomenon, and even though the specific regulatory, political, and cultural expectations placed on FIs differ in each country, one trend is consistent: the pressure is increasing to ensure customers are fairly treated.

On one hand, FIs are being required to defend their practices and demonstrate these practices are in the best interests of the customer. At the same time, revelations of inappropriate activity in large global FIs—involving market manipulation, rate fixing, mis-selling of products (e.g., purchase-protection insurance), and selling inappropriate products to seniors and the vulnerable—have resulted in greater regulatory attention to what guidance, rules, and requirements should be in place to help FIs do the right thing.

Canada is in the midst of the regulatory review process led by the Financial Consumer Agency of Canada (FCAC) and joined by the Office of the Superintendent of Financial Institutions (OSFI). All D-SIB banks and several other large FIs have been actively engaged in this review. They're having discussions on topics such as sales approaches, tone from the top, compensation and rewards frameworks, risk assessments, front line controls—essentially, any and all factors affecting retail sales practices. The regulators plan to release their industry review in 2018 as they report their findings and recommendations to the federal Department of Finance.

All regulated FIs should be considering how the intersecting drivers of conduct issues interrelate and how to enhance these drivers to demonstrate to their stakeholders how achieving good outcomes for clients is at the heart of their business model. This could include reconsideration of compensation models, enhancing board oversight, changing hiring practices, and changing the way customer outcomes are measured. More seriously, an FI that's found to be allowing misconduct to occur undetected could suffer significant reputational damage that could affect its business value, regulatory ratings, and customer trust.

Innovation for better customer outcomes

Clients need to feel they are being dealt with in a clear and open manner, with their best interests at heart. This can be a challenge when trying to explain complex financial matters. Consider the following example of an in-branch investment advisor–client relationship.

The bank's existing conversation script—designed to achieve certain compliance outcomes related to conduct legislation—had resulted in a complex conversation for bankers to manage, a poor experience for customers to navigate, and a sharp decline in branch sales performance.

To correct this situation, the bank built on a hypothesis developed from conversation theory and research insights to develop a prototype conversation model and simplified approach to compliance. Following initial concept testing, live testing was conducted with bankers in three varied branches over a period of seven weeks.

Over this test period, the quality of conversations improved, time to competency was reduced, sales performance increased, and compliance activity shifted from 'box-ticking' to more natural and authentic interactions design to achieve the best outcome for customers.

Insights from the initiative included:

- Scripted conversations based on legal and compliance requirements confused customers.
- Customers wanted interactions to be a continuous conversation rather than multiple exchanges.
- Small refinements in banker behaviour based on research insights led to significant changes in their interactions with customers.

From insight to action: boost your culture, conduct, and compliance approach

To improve your approach, consider taking the following actions:

- **Develop** a definition, whether broad or narrow, of conduct risk that suits your organization's unique situation. It should take into account regulatory jurisdiction, products, business model, and culture.
- **Build** an inventory of conduct vulnerabilities to which you are exposed.
- **Investigate** how to acquire data that helps you measure customer outcomes, not just customer satisfaction.
- **Monitor** customer complaints and determine escalation points and root, cause analysis.
- **Engage** all related stakeholders in your conduct risk conversations; for example, bring human resources in to review whether compensation structures could privilege heavy selling over customer fairness.
- **Investigate** whistleblower allegations and watch for patterns.
- **Focus** on the dictum "culture drives conduct," particularly in areas where culture is not aligned with intended outcomes.

Digital compliance

As the financial services industry becomes increasingly digital—enhancing offerings and changing the nature of customer interactions—compliance issues become more complex.

Dealing with that shifting dynamic is what digital compliance is about. Technology has historically not been a source of competitive advantage for the compliance function, but that will have to change significantly to manage increasingly digital compliance mandates. And it will be a wholesale change, involving both processes and people.

A number of challenges and impacts will arise as this shift continues, the position of regulators being a critical consideration. No matter how excited the industry gets over innovations like automated tools and artificial intelligence, the pace of change needs to be managed against regulatory expectations, what's safe for the customer, and what's safe for the bank. The question, then, is: as digital banking proliferates, to what degree and how quickly can regulation embrace, align and incorporate innovation. To understand the impact these changes are having on the industry, FIs and regulators will need to develop a close relationship that serves the interests of both parties and ultimately acts in the best interests of the end customer.

Digital compliance *is* innovation

It's difficult to talk about how innovation relates to digital compliance since the notion of building digital compliance competencies is really nothing *but* innovation. It's important to note, however, that different organizations are approaching the transformation imperative in different ways. Some are treating digital compliance as a full-scale transformation journey—an iterative process designed to achieve an ideal end state and carefully aligned with the speed of digital change at the business. Others are taking a pilot project approach, creating a test case in which innovative tools and technologies are incorporated into compliance processes to gauge their effectiveness. By starting small and creating a working proof of concept, successes can then be applied to other areas of the compliance function in incremental stages.

From insight to action: key steps along the digital compliance journey

A number of steps are involved in reaching your destination:

- **Implement** effective governance, including mechanisms to enable compliance decision-making in a fast-paced, innovative, and digital environment.
- **Improve** the agility, speed, and efficiency of processes to achieve compliance mandates. Consider adopting real-time, automated, intelligent risk management.
- **Enhance** technology and data capabilities, allowing the function to become innovative, relevant, and forward-looking, to partner more effectively with other functions, and to deliver enterprise-wide digital compliance solutions.
- **Develop** relationships with key external stakeholders, including regulators and industry groups, and bring them along on the digital journey.
- **Acquire** the appropriate multi-disciplinary talent resources to enable the speed, agility, and innovation your digital mandate requires.
- **Develop** mechanisms to communicate effectively in fast-paced, non-traditional digital environments, including not only among the compliance teams but also with the business functions, regulators, regtech and fintech companies, and other key stakeholders.

Where does Canada sit on the digital compliance curve?

A number of global banks are moving toward a focus on effectively using technology in the compliance function, but Canada's institutions aren't there yet. Some are making targeted strides, but there's no shining example. Nonetheless, achieving digital compliance is a true business imperative. Functions that focus on the current state, or even the past, risk seeing their overall value to their business partners and the organization itself diminish.

Payments modernization

Payments modernization refers to Payments Canada's goal of improving the speed, flexibility, security, and innovative focus of the Canadian financial system, which will ultimately result in strengthening Canada's global competitive position.

The out-of-date system now in use will be replaced by a system designed for faster, data-rich payments through new channels and services, and for the 24/7/365 payments capabilities clients are asking for.

Other improvements expected from the new system include reduced payments risk, automated legacy payment mechanisms such as cheques, improved transparency into transaction status information for payees and payers, fewer of the challenges currently associated with making cross-border payments, and the automation of certain aspects of electronic payment oversight. It's also expected ways will be found to enable fintechs and non-bank service providers to participate in shaping the future payments agenda.

Payments Canada released its payments modernization agenda in 2015, with a 2020 implementation vision. The Canadian Bankers Association supports this plan, and all participating FIs will need to implement the agenda's suggested changes for it to happen. That said, 2020 is not a firm date and these standards are not mandatory. Indeed, there is work left to do. While Payments Canada has released a modernization roadmap, it's still working to understand all the potential implications and risks, as well as consulting with FIs to understand whether proposed implementation timelines are realistic. Even when a firm timeframe is set, it's expected these capabilities will be implemented in a slow, scaled manner.

The impact on individual FIs depends on whether Canada moves forward effectively or falls behind in its implementation goals. If some FIs decide not to participate, for example, this could put them at a significant disadvantage. However, given the tremendous advantages to be gained, mass participation is highly likely.

If all the parties do participate, they'll have much to do. For example, all the platforms used to authorize, settle, and reconcile transactions—including cheques, cash, wire, and electronic transfers—will have to be upgraded to meet the technological requirements of the modernization agenda.

Given that close to one billion transactions will be migrated from legacy systems onto the new platforms, significant infrastructure investments will be required. On the upside, since future transactions may be cleared and settled in real time, banks might be able to reduce the amount of money they traditionally hold in their capital reserves for end-of-day settlement, which could in turn offset anticipated infrastructure modernization costs.

Also, with over 40 countries already modernizing their payments infrastructure and moving to the emerging ISO 20022 standard, Canada's FIs will be able to participate more effectively in the evolving global payments ecosystem, again helping us to stay engaged and competitive. Consumers will clearly see enormous benefits, with 24/7/365 payments capabilities enabling the instantaneous moving and clearing of money. Consider the e-transfer: even though it was introduced as a real-time service, there was initially a 20-minute delay due to perceived fraud risks. This delay may now be eliminated.

Innovation will be the cornerstone of payments modernization

A vast increase in transaction speeds is now possible thanks to technological innovation. However, further advances will be required to address some of the potential negative repercussions of this speed. Real-time transacting may provide benefits around liquidity and capital, but it can also increase the risk of fraud, money laundering, and other financial crimes. It's happened in other jurisdictions: when faster payments were implemented, criminals targeted back-end systems that weren't yet upgraded to function at the same speed. When Canadian FIs implement real-time transactions, they'll have to be sure that real-time decisions on fraud and money laundering can be made as well, and that fraud-related compliance requirements for systems, governance, processes, and controls are updated. Otherwise, the risk of significant loss could be high.

From insight to action: preparing for the payments revolution

Focus on keeping your clients' money safe during transactions, for now and tomorrow:

- **Strive** to maintain the safety, soundness, and resiliency of your transactions environment. The current environment is secure and the risks well-known, so FIs must introduce new features—and deal with accompanying new risks—in a highly managed, measured, and controlled environment.
- **Determine** the gains the new system will bring in terms of efficiency and effectiveness. What are the implications of enabling faster, more data-rich payments, and how can the organization best enhance value?
- **Focus** on meeting client needs while still protecting them from risk. FIs are not fintechs and will need to balance their more conservative risk postures with the many client benefits the payments modernization agenda is sure to enable.

Canada is taking action on transaction trends

Numerous transaction trends are taking hold in Canada. One of the top trends is the increasing use of credit and debit cards over cash, much of which is being driven by contactless payments capabilities. In fact, the move toward electronic payments is faster than that of our US counterparts, though probably not faster than Europe. Smartphone ownership is rising as well, which will be a prime enabler of new digital payment choices and channels. This electronic impetus bodes well for the payments modernization agenda, and the country appears primed to take the next steps toward adoption.

Cyber risk

A pivotal cyber risk-related regulatory issue for the coming year will be the General Data Protection Regulation (GDPR).

This European Union (EU) legislation, set to come into force May 25, 2018, sets ground rules and provides guidance about how organizations need to handle and protect the personal data of any individuals in the EU. The GDPR will affect Canadian FIs that have EU operations and/or process the personal data of EU-based customers or employees.

It is this extraterritorial scope, alongside extended rights to the individual, that makes GDPR unique amongst global data protection laws. Many FIs are well on their way to defining their compliance programs and by now are entering the last mile to be aligned with GDPR by May 2018.

GDPR sets a new international bar when it comes to regulatory expectations regarding the protection of privacy. It clearly reflects the direction of both public and regulatory sentiment, and all organizations must understand these implications, including Canadian FIs with operations in Europe. For example, affected FIs will need to provide customers with significant new information concerning what is being done with their personal data (e.g., automated profiling and possible transfer of personal data due to use of foreign service providers) as well as the security initiatives in place to protect it. Organizations must also provide customers with greater control over how their data is used, meaning individuals can give or withhold consent for generic or specific uses.

There are also new requirements that, until now, have only been adopted as best practices. These include making it mandatory for organizations to protect privacy by design and by default, conducting data-protection impact assessments, appointing a data protection officer, and keeping records of data-processing activities. Additionally, there are greater expectations about the security measures organizations must have in place, meaning many will have to do things like bolster controls concerning encryption and pseudonymization of data, review the maturity of their existing cybersecurity program as well as their business continuity and breach response programs, and ensure that existing controls are regularly tested to evaluate their effectiveness.

The most critical aspect of GDPR is that it's far more customer-centred than past laws. It puts unprecedented control into the hands of individuals. FIs will need to implement enhancements to current processes and technical functionality in order to support the expanded rights of individuals.

Innovation and the GDPR

The implementation of legislation that changes the way data is handled will require a significant amount of technological innovation, such as for the digital management of individual rights and consent options. Both automation and RPA can help organizations better streamline their control set. FIs will also need to better understand the systems they use to collect, process, store, and disclose data across the personal data lifecycle. Most organizations only realize their innovation approaches have holes when a breach happens. However, by considering the right controls and technologies prior to implementation—by understanding things like what data they have, who owns it, which departments have access to it, and where it's kept in the systems—FIs can strengthen their privacy and security posture while they innovate, putting them in a better position to respond to disruptive market forces.

From insight to action: how FIs should be preparing for GDPR implementation

The new legislation needn't be onerous, but you should be ready for May 25. Here's how:

- **Complete** readiness assessments and ensure you're well on your way to implementing control activities that demonstrate an understanding of GDPR, put a detailed roadmap in place, and prioritize controls against high-risk areas.
- **Review** existing policies and processes, make any necessary technology changes, get documentation requirements in order, and appoint the right people to execute these tasks after completing assessments.
- **Enable** privacy by design by ensuring privacy is built into the program's full lifecycle at the earliest point of any initiative in which personal data is handled, such as developing a new process or designing a system. Implementing privacy by design will also help ensure that privacy is protected by default. This means, for instance, that customers wouldn't have to change the privacy settings of a solution since these would be designed to be switched on by default.
- **Understand** changing breach requirements and be able to respond effectively. For example, update the existing breach response plan and breach notification requirements in third-party contracts to ensure you can meet the 72-hour deadline to notify supervisory authorities.
- **Appoint** a data protection officer, and a European representative when appropriate, to confirm that all activities related to privacy are properly documented and maintained over time.
- **Assess** the gap between GDPR requirements and your technology capabilities. Then prioritize and sequence the changes required by executing a risk and cost/benefit analysis.
- **Develop** a heightened awareness of privacy and the importance of data protection among employees; the right culture will help ensure employees are handling data in both legally and ethically compliant ways.
- **Train** customer-facing staff to respond to specific customer questions about how their data is being handled, and how it is being shared, protected, etc.
- **Set up** and **undertake** regular compliance audits or reviews to ensure the GDPR program at your organization is being effectively implemented and sustained in the long term.
- **Increase** focus on transparency by preparing to share details regarding the purpose of collection, the intended use, and the manner of disclosure for all kinds of information, so customers fully understand when they consent to something.

Canada and the GDPR

As GDPR comes into effect, Canadian FIs with EU operations and/or that process the personal data of individuals in the EU will need to fully understand the impact of the regulation on their operations and make enhancements to their privacy and security programs. The penalties for non-compliance will be the heaviest in the world—up to four percent of annual turnover for significant violations—and EU regulators will have greater enforcement powers than their Canadian counterparts. Despite the effort required, these privacy and data protection laws should be seen as a competitive boon: if its compliance is full and effective, an organization can differentiate itself as a leader in the evolution of data privacy.

Risk operations

The risk operations function in many FIs is currently repositioning itself to better manage anticipated challenges.

The bureaucratic risk management function of the past is disappearing. Its future incarnation will be different, focused on developing insights to help the business make more risk-informed, strategic decisions. Indeed, this must happen if the function is to cope with the innovation underway in the financial services industry and the new risks it will bring. On the other hand, dealing with the recent pressure from new industry entrants, new technologies, and the rapid pace of regulation has made the function inefficient and slow to respond to change. Not only must risk change its focus, it must also be streamlined so that focus can be efficiently and effectively executed.

Many factors are driving this transformation imperative, including market volatility, business and structural change, the need for data accuracy, and rapidly evolving regulatory requirements. To the last point, it's worth noting that—while there are numerous risk regulations—overhauling the function itself is not a regulatory requirement. The objective is not to survive the regulators but to more nimbly support and challenge the business in order to drive organizational value.

Trimming the risk function to operate more leanly and keep pace with innovation has been a challenge. Measures to improve the function have tended to be reactive rather than proactive, but with pressure building to do more with less, change must become more active. This will have certain impacts. To become more efficient and effective, the function needs to consider new techniques, tools, and technologies. It must also re-evaluate the organization's governance structure, particularly the three lines of defence: the roles and responsibilities of the business units, the risk and control functions, and internal audit. Effectively done, these efforts can speed up the pace of change and the ability to innovate. Poorly done, risk management capabilities could decline, exposing the organization to financial loss and fines.

Innovation in risk operations

Innovation takes on a particularly paradoxical aspect in the risk function context. It's critical to enacting change within the function—for example, improving efficiency by automating where possible and removing manual tasks. This fits in as part of improving operations through technology. The flip side is that, along with the rapid pace of change, innovation itself brings new risks. Therefore, having risk management deeply involved in any innovation initiatives—including its own—is essential to ensuring the company will thrive well into the future. Leading organizations are taking this tack, embedding risk into all strategic initiatives in order to compete more effectively.

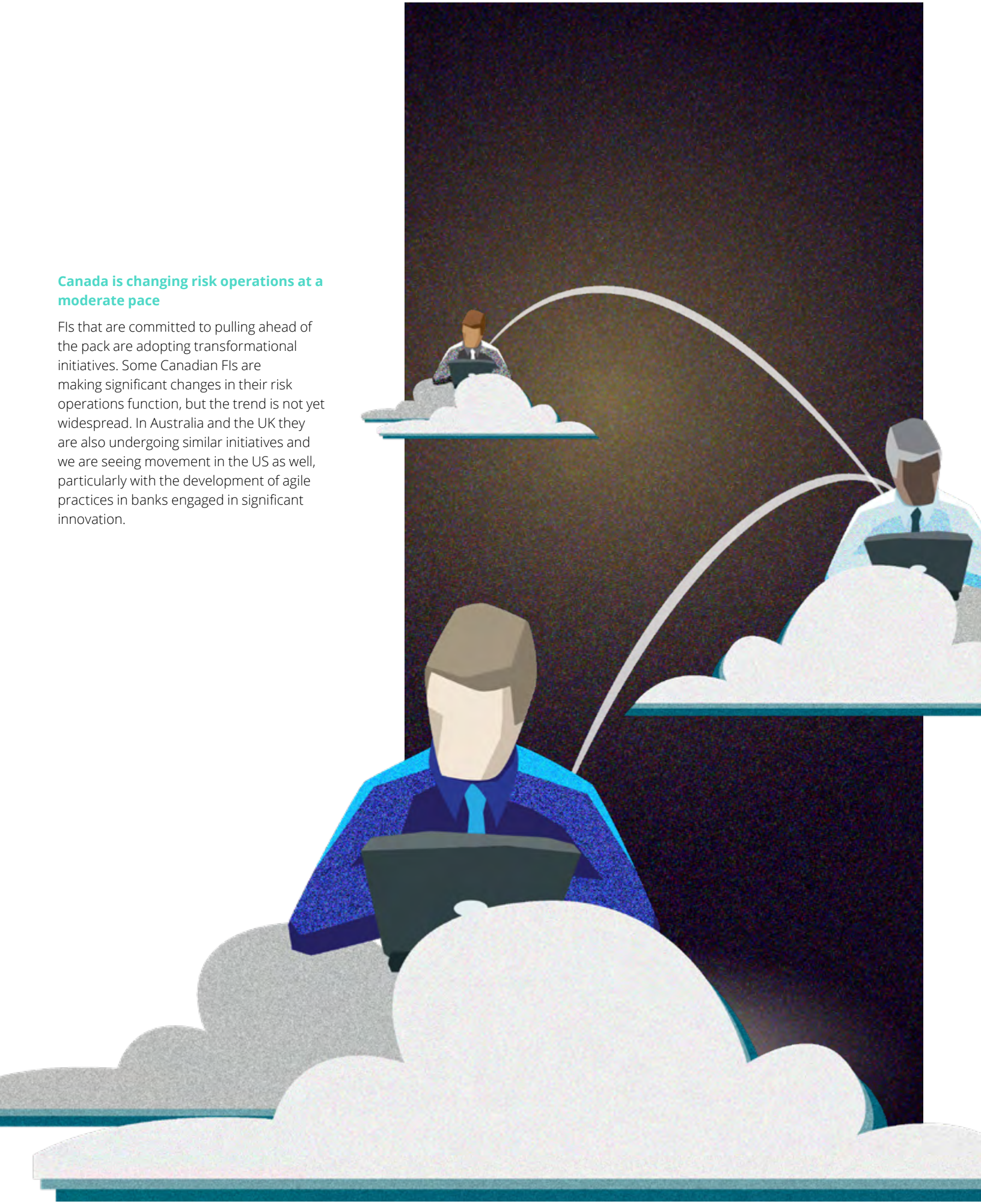
From insight to action: How to transform risk operations

Consider these steps to improve your operations. You can:

- **Streamline** the three lines of defence to reduce duplication and overlap of responsibilities, as well as address gaps between them. Duties need to be segregated, but the lines need to ensure they're using similar terminology, that handoffs and sequencing are appropriate, and that ownership of responsibilities is clear. Look at these three lines as a whole rather than as separate entities to better understand how risk applies across the various control partner groups.
- **Re-envision** the risk operating model. In this instance, the focus is on finding opportunities for efficiency in the risk function. Explore techniques to free up capacity and reduce costs. Consider improving the interaction model, streamlining processes, implementing automation, and taking a fresh look at talent, including recruiting, onboarding, and retention issues.
- Better **integrate** risk management into the delivery of projects and new innovation. For example, agile project management practices require rapid and decisive interactions, but many risk functions are not set up to support such an approach and often become a bottleneck rather than an effective control function.

Canada is changing risk operations at a moderate pace

FIs that are committed to pulling ahead of the pack are adopting transformational initiatives. Some Canadian FIs are making significant changes in their risk operations function, but the trend is not yet widespread. In Australia and the UK they are also undergoing similar initiatives and we are seeing movement in the US as well, particularly with the development of agile practices in banks engaged in significant innovation.



Building resilience through innovation

There is no question the established order is shifting rapidly—financial services organizations are facing change, and a range of accompanying risks, on an unprecedented scale. While the industry has traditionally managed core financial risks effectively, organizations must increasingly be alert for new areas of risk and embrace new and innovative methods by which they can stay ahead of the changing risk profile of their business model.

This can be a challenge when, given current market conditions, the drive to cut costs and improve the bottom line can put pressure on risk management resources. Despite these pressures, organizations must find a path to resilience, identifying ways to manage traditional emerging risks while doing more with less and driving competitiveness. The innovative mindset needs to permeate organizations' risk management function as well as their strategic thinking. And regulatory risk—as this report makes clear—is no exception.

Rapid change continues to be a defining force in today's economic, business, and technological environments. Organizations that foster and capitalize on innovation to manage both financial and non-financial risk in better, faster, more cost-effective ways will be the first to recover from adversity, realize a competitive advantage, and clearly differentiate themselves in the market.

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

Paul Skippen
Partner, Risk Advisory
416-874-4411
pskippen@deloitte.ca

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

Robert Cranmer, Director, Risk Advisory
Ray Westcott, Director, Financial Advisory
Michael Abate, Senior Manager, Risk Advisory
Jas Anand, Senior Manager, Risk Advisory
Sandeep Chopra, Senior Manager, Risk Advisory
Matt Devine, Senior Manager, Risk Advisory
Beth Dewitt, Senior Manager, Risk Advisory
Aneesa Ruffudeen, Senior Manager, Risk Advisory
Betty Tien, Senior Manager, Risk Advisory
Irene Sanchez Reverte, Senior Consultant, Risk Advisory

CENTER *for*
REGULATORY STRATEGY
AMERICAS

About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

Deloitte.

www.deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 17-5259M