Office of the Superintendent of Financial Institutions Canada
Bureau du surintendant des institutions financières Canada

Non-Financial Risk and Operational Resilience: The Rise of Machines

Remarks by Assistant Superintendent Ben Gully prepared for the C.D. Howe Institute

Toronto, Ontario
February 7, 2019

For additional information:

Brock Kruger
Communications and Consultations
brock.kruger@osfi-bsif.gc.ca
www.osfi-bsif.gc.ca

OSFI BSIF

Canada

Remarks by Assistant Superintendent Ben Gully
Office of the Superintendent of Financial Institutions (OSFI)
Prepared for
C.D. Howe Institute
Toronto, Ontario
February 7, 2019

Introduction

Thank you for inviting me to be here today.

Financial institutions are lifting their business capabilities through a powerful combination of new technology and rapid digitization. These developments are fundamentally altering their operating environment and the expectations for effective risk management.

Looking ahead, it is only creativity and imagination that will give us an idea of where it all may lead, but it is human judgement and effort that will make it happen.

Technological advancements point toward a promising future. For financial institutions, fulfilling promises is how they build and maintain their reputations. From a prudential perspective, OSFI is interested in how financial institutions adapt and respond to technological changes. For example, we are interested in how they manage and mitigate operational risks posed by these new advances.

Critically, our shared interest lies in how these risks may affect trust and confidence – or "reputation" of financial institutions because without it, financial institutions will struggle.

Today, I will illustrate three areas where OSFI is paying particular attention to how technology and digitization are affecting operational risk at financial institutions: (1) the use of advanced analytics such as artificial intelligence or machine learning; (2) the spread of third-party service providers; and (3) the evolution of information security for cyber threats.

OSFI is making internal changes to respond to these so-called 'non-financial risks'. We are building new capability and infrastructure to address the supervision of operational resilience as a key component of financial safety and soundness. It is our responsibility to share our views on what we know about the steps financial institutions should be taking to improve their resilience in an increasingly technological and digital world.

Changes to business and operating models at financial institutions

In today's environment, financial institutions are increasingly collaborating with technology companies to leverage new technologies – also known as "fintech". These changes are important, promise certain efficiencies and offer new capabilities to business management.

But make no mistake; they also have the power to fundamentally alter the business and operating model of a bank or insurer.

Some opportunities come in the form of white-labelling strategies where a financial institution relies on its partner for the acquisition of customers; in other words, no need to face the customer.

Other opportunities may include accounting software, payroll services, basic legal advice or venturing into new fee-based services focused on a platform model. These are all steps away from traditional business models.

Operating models for financial institutions are also changing dramatically. The availability of open IT systems rather than typical legacy IT systems, tech-driven automation and the ability to deploy programs that compress technology development cycles are all changing the choices institutions are making. These choices are bringing products and services to market at a frenetic pace.

Technology will enable or accelerate further decentralization of financial market participants and blur the boundaries of a traditional regulated financial institution. The decentralization both magnifies non-financial risks and diffuses accountability: the former must be mitigated by specifically designed controls while the latter runs counter to the foundation of OSFI's B-10 guidance – namely that accountability remains with the financial institution, regardless of the third party arrangement.

The safety and soundness of financial institutions will depend, in part, on the ability of risk management functions to develop and maintain understanding and control of its enterprise in in a broader ecosystem of partners. Such shifts in risk management will support a better understanding of non-financial risk in a tech-driven environment and enable institutions to ensure accountabilities for risk-taking remain clear and transparent. This in turn will help them to become more resilient to operational disruption.

We have seen the link between non-financial risks and their impact on reputation, such as the public and stakeholder responses to third-party privacy breaches. These can quickly affect an institutions' operations, its ability to grow its business and potentially its bottom line.

In our view, traditional financial resilience measures for risk managers and regulators such as available capital and liquidity, are necessary. They are more easily quantifiable and generally understood as a source of strength by markets and investors. However, they may not be enough to manage non-financial stress; indeed, they are likely inadequate responses to operational disruption for which there are fewer "tangibles" to measure.

A broader perspective to resilience is therefore required for OSFI and the financial institutions it supervises; one which considers the anticipation, prevention, detection, response and recovery from operational risks.

Advanced Analytics

According to the World Economic Forum (April 2018), more data has been created during the past two years than the previous 5,000 years, and this number is on the rise according to other predictions. Big data is big business.

While the use of data analytics is not new, the growth of computer power is transforming the ability to analyze more and increasingly diverse sources of data.

Financial institutions are using big data across a wide range of applications, including credit risk measurement and management, fraud detection, pricing, investment portfolio optimization, client interaction and customer advisory services … and the list goes on.

Big data combined with artificial intelligence and machine learning is already going well beyond the traditional business intelligence tools. These advanced analytics can help to gain deeper insights into customer behaviours, to make predictions or to generate recommendations for decision-making.

This is valuable but not without risk. There are risks related to data quality and model-risk governance issues, risks stemming from compliance with consumer protection rules as well as possible data privacy concerns that could pose legal and reputation risks to financial institutions.

Advancements in risk analytics are welcome and important but they require new capabilities in risk management. Machines using more data can offer greater prediction and efficiency. In fact, machines can help improve detection of problems and reduce costs. But when machine learning is used at the expense of transparency or trust, there is a need for even greater human intervention and more effective challenge. Without it, the legitimacy of machines and the institutions that employ them will be undermined.

At OSFI, we are also improving our own tools, staffing and training to meet the future. This is also an opportunity to experience digital transformation ourselves. Doing so is essential for OSFI to continue to hold financial institutions to a high standard and to evaluate their oversight of advanced analytics, including the use of Artificial Intelligence and Machine Learning.

We are guided in this by fundamental principles related to model risk governance that preserve transparency and ultimately, the perceived legitimacy of analytical outcomes.

Third-Party Ecosystem

Financial institutions are increasingly looking to third-party providers – via advancements in technology – to help them take advantage of efficiency and scale. The so-called ‘third-party ecosystem’ is growing fast and is increasingly diverse, which means the boundaries of a traditional financial institution are becoming increasingly porous.

Critically, some of these third-party arrangements clearly fall outside of OSFI's classic definition of an outsourcing arrangement.

Traditionally, financial services clients had a lot of bargaining power and could insist on customized master services agreements. With cloud computing and other scaled solutions, third-party service providers can insist on a "one-size-fits-all" model. The move toward standard terms may mean a financial institution has less control over services. As well, these third-party providers remain unregulated in many jurisdictions.

The concern here is that risks third parties experience can spread quickly to their partners by disrupting operations and negatively affecting the reputation of the financial institution.

While third parties offer advancements in capability, they can challenge transparency for risk management. As a result, OSFI continues to expect financial institutions to understand and manage the risks of their third-party arrangements.

We expect institutions to assure themselves of the quality of risk management practices within the third party and the implications that this may have for their operational resilience.

With the growth in third-party relationships, risk concentrations may result when a number of financial institutions' begin to rely upon a few service providers. OSFI's concern is that the dominance of a particular supplier in one area could create a co-dependence across the financial services sector. This matters because financial system resilience would ultimately rely on the operations of a potentially small number of non-financial, technologically driven, counterparts.

In preparing for the severe but plausible event in the non-financial risk environment, OSFI is gathering information on the types and extent of financial institutions' dependencies on third-party service providers.

As part of the scope of this work, we will be focusing on operational resilience, cloud technology and information security. This will not be a "once and done" review and our work will continue as the third-party ecosystem evolves.

Cyber Security

With growing volumes of digitized data and improved access to it through new technology, there is a growing potential exposure of information security to cyber risk.

An institution's cyber resilience depends upon its ability to effectively detect, respond and recover from inevitable breaches. The relentless pace of change and persistence of threats requires continual improvements to cyber risk management practices.

Many of the cyber attacks reported to date have been via the digital banking channel – fraudulent payments, phished or stolen credentials email phishing and automated account takeovers. Financial institutions need to consider their third parties as a source of risk and potential liability, too.

There is no magic in what makes an institution resilient to cyber risk. Operational resilience to cyber threats includes securing the organizations perimeter, using secure configurations, user access control, malware protection and patch management and the list goes on.

These actions may sound basic but even simple cyber hygiene has increased an institution's effectiveness in managing potential threats. Regularly changing passwords, ensuring only privileged access to critical information and carrying out regular penetration testing go a long way to promoting resilience and continuous improvement.

These measures are only part of the solution. Little is accomplished through improved preventive measures if no thought is put into how to recover when an event occurs.

We will continue to monitor financial institutions' ability to self-assess and respond to cyber incidents. Operational resilience testing by firms will be key and we know that we have work to do on building our tools and techniques in this area.

OSFI is refining its own internal cyber incident response protocol as well as coordinating and collaborating with the New Canadian Centre for Cyber Security in preparation for a potential national security incident.

By increasing the number of players engaged in cyber security, we are spreading the load to match the spreading of risk. Together we have a better chance of using the data and analytics from these events to improve upon how we all identify and respond to these threats.

OSFI's Response

It has been 10 years since the global financial crisis and the response to making the system more resilient to financial stress has been substantial. However, we are at a crossroads in risk management and supervisory oversight.

While we need to be maintain our focus on financial resilience, we also need to shift thinking toward the risk management of other non-financial risks because more capital will not improve resilience against a cyber attack or the service interruption of a third party.

New tools for newer risks will be required for risk management at financial institutions. OSFI is working hard in building out these new tools and laying the groundwork for collaboration with other experts, both domestically and internationally.

We are discussing and assessing good practices around operational resilience to non-financial threats. By improving our own understanding, we are better able to supervise and respond to the risks that institutions are facing. Our goal is clear: to establish a common understanding around what constitutes effective risk management within a technologically mature world.

Conclusion

There are number of ways to view the future.

Technology promises access to new business and efficiency gains that are an important part of continued success, innovation and financial stability.

By only focusing efforts on gains, there is a real threat that risks will go unidentified or unaddressed and financial institution reputation will be undermined.

Machines are making the business more productive and capable; however, human judgement will continue to define the overall effectiveness of risk management for the foreseeable future.

What is different now than in the past is how far we can see into the future. It is shortening given the pace of technological developments and digitization.

Keeping an open dialogue with risk practitioners, technology and data science experts as well as other expert stakeholders is key to creating our own future stability. I am glad to have had the opportunity to be here today and look forward to continuing dialogue on this important area.