

DISCUSSION NOTE

From Spreadsheets to Suptech

Technology Solutions for Market Conduct Supervision

JUNE 2018



WORLD BANK GROUP

Finance, Competitiveness & Innovation Global Practice

© 2018 International Bank for Reconstruction and Development / The World Bank

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

RIGHTS AND PERMISSIONS

The material in this work is subject to copyright. Because the World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Any queries on rights and licenses, including subsidiary rights, should be addressed to the Office of the Publisher, The World Bank, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2422; e-mail: pubrights@worldbank.org.



CONTENTS

Acknowledgments	ii
Abbreviations	iii
1 INTRODUCTION	1
2 UNDERSTANDING SUPTECH	2
2.1 Suptech versus Regtech: What's in a Name?	2
2.2 Suptech for Market Conduct: Potential Use Cases and Outcomes	3
3 SUPTECH IN PRACTICE: MARKET CONDUCT CASE STUDIES FROM THREE COUNTRIES	6
3.1 Case Study: U.S. Consumer Financial Protection Bureau	7
3.2 Case Study: Bank of Lithuania	10
3.3 Case Study: Central Bank of Brazil	12
4 CROSS-CUTTING CONSIDERATIONS	15
REFERENCES	18
BOXES AND FIGURES	
Box 2.1 Automated Data Collection in Austria and Rwanda	5
Box 2.2 Exploring Machine Readable and Executable Regulations in the United Kingdom	5
Figure 1 Suptech Conceptual Framework	6
Figure 2 Bank of Lithuania's Electronic Complaints System	11
Figure 3 Scope of Risk-Assessment Exercise for FSPs	12
Figure 4 Central Bank of Brazil's Conduct Risk Framework for NBFIs	13
Figure 5 Central Bank of Brazil's Conduct Inspection Workflow for NBFIs	14



ACKNOWLEDGMENTS

This discussion note is a product of the Financial Inclusion, Infrastructure & Access Unit in the World Bank Group's Finance, Competitiveness & Innovation Global Practice.

This note was prepared by Gian Boeddu, Laura Brix, Nomsa Kachingwe, Ligia Lopes, and Douglas Randall. Mahesh Uttamchandani, Douglas Peace and Sebastian Molineus provided overall guidance. The team is grateful for the substantive feedback received from peer reviewers Sharmista Appaya, Denise Dias, Erik Feyen, Juan Carlos Izaguirre, Ivo Jenik, and Mark Schrijver.

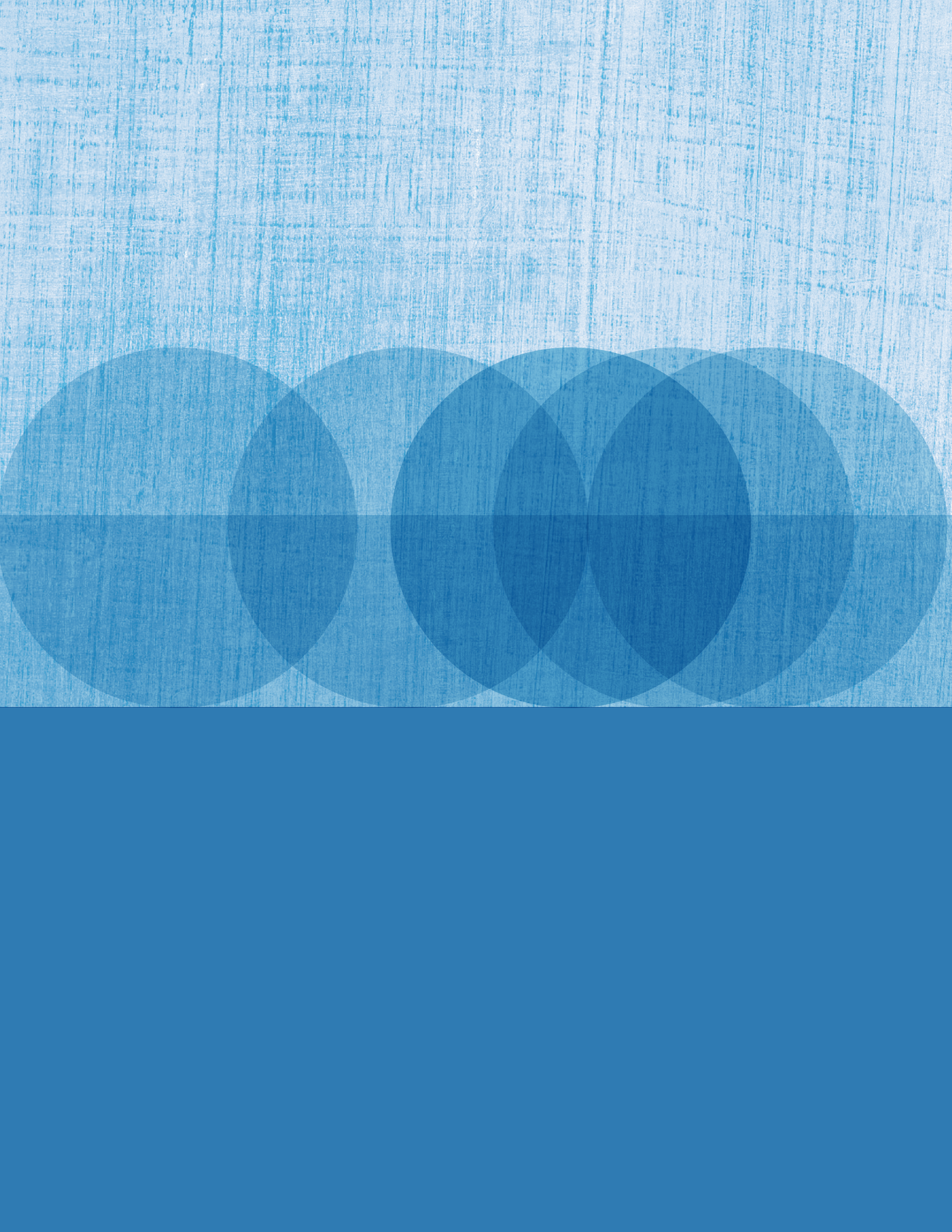
The team gratefully acknowledges the generous contributions of time and expertise by financial sector authorities at the Consumer Financial Protection Bureau (United States), the Bank of Lithuania, and the Central Bank of Brazil.

The team thanks Naylor Design, Inc. for design and layout assistance, and Charles Hagner for editorial inputs.



ACRONYMS AND ABBREVIATIONS

AML/CFT	anti-money laundering/combating the financing of terrorism
BCB	Central Bank of Brazil
BoL	Bank of Lithuania
CCD	Consumer Complaint Database
CFPB	Consumer Financial Protection Bureau
CRM	customer relationship management
Fintech	financial technology
FSP	financial service provider
NBFI	nonbank financial institution
Regtech	regulatory technology
SisCom	Integrated System for Supervision Support and Communication
Suptech	supervisory technology





1 INTRODUCTION

Effective and efficient market conduct supervision is critical to ensuring that financial consumers are protected from unfair business practices and provided with clear and relevant information. In countries with ambitious financial inclusion agendas, robust market conduct supervision is important to ensure that financial inclusion objectives are achieved responsibly and sustainably. Maintaining the integrity of the financial system is also sometimes considered as an aspect of market conduct supervision.

Yet market conduct supervision is a challenge in many jurisdictions. Effective market conduct supervision requires the collection of a wide range of data from disparate sources. Financial sector supervisory authorities (supervisory authorities) must also undertake complex, qualitative analyses to determine compliance with legislation or regulation that is often principles based or comprises judgement-based rules. These challenges are compounded when a financial sector supervisory authority's market conduct mandate covers a large number and a diverse range of financial service providers (FSPs), and when many such FSPs have unique or unfamiliar risk profiles. For example, a supervisory authority's mandate may cover not only commercial banks but financial cooperatives, microfinance institutions, nonbank e-money issuers, and new Fintech (financial technology) market entrants such as person-to-person lending platforms. Supervisory authorities may also face capacity constraints, particularly in cases where the market conduct supervision function is at a nascent stage or is inadequately staffed or funded.

Many supervisory authorities are therefore seeking technology-enabled solutions to increase the efficiency and effectiveness of their supervisory activities. The use of technology can enable supervisory authorities to better identify and monitor sources of risk and improve the accuracy and timeliness of information flows and interactions between the supervisory authorities and financial sector

stakeholders. The use of technology to facilitate and enhance supervisory activities and processes is referred to in this discussion note as Suptech (that is, supervisory technology).

This note highlights examples of technology solutions that are being adopted for market conduct supervision, including the implications of these technology solutions for broader supervisory approaches. The term *market conduct supervision*, as used in the note, refers to aspects of financial sector supervision other than prudential supervision, such as consumer protection, anti-money laundering/combating the financing of terrorism (AML/CFT),¹ and competition-related business conduct issues. Suptech approaches to market conduct supervision are in some ways similar to those pursued for prudential supervision, although there are also importance differences, as will be discussed in this note.

The note provides a general examination of Suptech, as well as three country case studies. The note begins with a conceptual overview of Suptech and related concepts in section 2. This is followed in section 3 by three case studies that illustrate how Suptech is currently being applied by market conduct supervisory authorities—specifically, in the context of financial consumer protection (using country case studies from the United States and Lithuania) and in the context of AML/CFT (using a country case study from Brazil). Section 4 concludes with a discussion of cross-cutting considerations, including the risks and challenges that may arise with Suptech, and areas for further research and exploration.

As noted by the Toronto Centre, many examples of Suptech solutions, particularly those using the most

1. The Financial Conduct Authority (United Kingdom) and the Central Bank of Brazil are examples of authorities that refer to financial consumer protection, competition, and market integrity as conduct risks.

innovative technologies, are still at concept or pilot phase (Toronto Centre 2017, 12). Some of these are discussed in section 2. However, the case studies discussed in section 3 were selected because they involve the implementation of Suptech solutions in two different market conduct supervision areas and were sufficiently advanced in their implementation to allow an examination of the practical experience of the relevant supervisory authorities.² It is hoped that this note will provide useful lessons and insights on the opportunities and challenges for the use of Suptech to enhance market conduct supervision.

2 UNDERSTANDING SUPTECH

2.1 SUPTECH VERSUS REGTECH: WHAT'S IN A NAME?

The terms *Regtech* (that is, regulatory technology) and *Suptech* have recently emerged in discussions among financial sector practitioners. However, no definitions of these terms are universally agreed upon, and wide variation remains in how they are applied. This section provides a brief summary of different perspectives on Regtech and Suptech, and outlines the working definitions and conceptual framework adopted for this note.

Regtech

In many jurisdictions, increased scope and complexity of regulation has raised compliance costs for FSPs. For example, some FSPs are being subjected to new areas of regulation (for example, financial consumer protection), and others are being required to meet higher standards in existing frameworks (for example, with respect to risk data aggregation and reporting). Regtech is one response to these trends. Most definitions of Regtech focus on the use of technology to enhance FSPs' ability to achieve regulatory compliance while minimizing costs.

For example, the Institute of International Finance defines Regtech as "the use of new technologies to solve regulatory and compliance requirements more effectively and efficiently" (IIF 2016, 3). In the United Kingdom, the Financial Conduct Authority has described Regtech as "a sub-set of Fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities" (Woolard

2017). The relationship with Fintech³ is also evident in this definition from an industry participant: "[Regtech] is a term coined to classify a group of companies that, by harnessing the capabilities enabled by new technologies such as cloud computing, big data, and blockchain, are devising solutions to help companies across all sectors of activity ensure that they comply with regulatory requirements" (Fernández Espinosa 2016). Finally, the International Regtech Association describes Regtech as "digitization of regulatory compliance processes," which places the focus on automation and enhancing or eliminating manual processes (IRTA, "Supporting the Development").

While FSPs' regulatory compliance and supervisory authorities' supervision processes likely overlap, and some commentators have used the term *Regtech* also to refer to technology for use by supervisory authorities, this discussion note uses the term to refer to the use of technology to facilitate and enhance regulatory compliance processes from the perspective of FSPs.

Suptech

The increased scope and complexity of regulation that has raised compliance costs for FSPs also presents a challenge for the supervisory authorities who must process and analyze data of ever-increasing volume, frequency, and granularity. Greater market diversity and innovation further stress the capacity of supervisory authorities in many jurisdictions. In response, supervisory authorities are seeking to leverage technology and digitize key processes in order to increase their efficiency and effectiveness. While less attention has been given to defining and advancing the concept of Suptech relative to Regtech, interest in Suptech is on the rise.

The Basel Committee on Banking Supervision has defined *Suptech* variously as "the use of new technologies for internal supervisory purposes" and "the use of technologically enabled innovation by supervisory authorities" (BCBS 2017, 31). The Basel Committee elaborates on this concept by noting that "Suptech lets supervisors conduct supervisory work more effectively and efficiently. This differs from Regtech, as Suptech is not focused on assisting with compliance with laws and regulations, but on supporting supervisory agencies in their assessment of that compliance" (BCBS 2017, 35).

2. The descriptions of the implementations in this note were based on interviews with, and materials provided by, the respective supervisory authorities.

3. The Basel Committee on Banking Supervision (BCBS 2017) and Financial Stability Board (FSB 2017) define Fintech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services."

Thus, for the purposes of this discussion note, Suptech is used to refer to the use of technology to facilitate and enhance supervisory processes from the perspective of supervisory authorities.

Technology-enhanced supervision is not new, of course. Various technology solutions have been adopted by supervisory authorities over the years to improve the efficiency of supervisory processes and activities—for example, database management software, XBRL (that is, eXtensible Business Reporting Language), and other electronic reporting templates and tools to capture and analyze data.

Yet supervisory activities in many jurisdictions remain heavily reliant on manual processes. Unintegrated internal information-management systems and inflexible standard report templates also hinder the degree to which supervisors can identify and analyze risks in real time. And many supervisory authorities also struggle to make effective use of unstructured⁴ or qualitative data (such as information related to complaints, disclosure materials, annual reports, and so forth). Suptech solutions provide an opportunity for supervisory authorities to shift away from manual, unintegrated, “tick-box” processes to automated, real-time, integrated, and “smart” supervisory processes.

Many Suptech solutions include an element of process automation, which enables the automation of manual, rules-based processes like inputting or processing data across multiple platforms. An example of this would be a data-pull system that allows a supervisory authority to automatically access raw business data directly from an FSP’s management information system at predetermined intervals and to aggregate the data into a set of indicators and reports. A supervisory authority can also use process automation to integrate data from a range of sources (such as monthly off-site supervision returns, financial ombudsman data, and credit bureau data) into a single report.

Artificial intelligence offers further opportunities to improve the efficiency and effectiveness of market conduct supervision. Artificial intelligence tools can mimic human thinking, including by automating the process of discovering and testing hypotheses and extracting insights from data.⁵ For example, artificial intelligence can be applied to discover patterns of recurring friction points between providers

and customers through analysis of consumer complaints data. Artificial intelligence tools can also be leveraged in the analysis of suspicious transactions to identify those that warrant closer investigation.⁶

As a recent Toronto Centre note points out, the emergence of Suptech may enable broader shifts in approaches to supervision, toward “a pro-active, forward-looking supervision that relies on better data collection and sophisticated data analytics, and greater storage and mobility capacity” (Toronto Centre 2017, 10). While Suptech solutions need not always involve cutting-edge technology to be effective in achieving these goals, it is also important to continue to pursue innovative approaches so that supervisory authorities can fully leverage the benefits of technology.

2.2 SUPTECH FOR MARKET CONDUCT: POTENTIAL USE CASES AND OUTCOMES

The demand for Suptech solutions among market conduct supervisors is present and growing. To date, however, it appears that relatively few private sector providers—including Fintech companies and established technology service providers—have emerged to serve the unique needs of market conduct regulators and supervisors (Petrasic, Saul, and Lee 2016). Many of the basic tools used to undertake market conduct supervision are similar to those used for prudential supervision, as both types of supervision involve market monitoring as well as off-site and on-site inspections. However, the implementation of these tools often differs—for example, in the type of data collected, risks assessed, and corrective actions deployed. Market conduct supervision also typically includes a unique set of tools, including monitoring FSPs’ treatment of individual customers, assessing the effectiveness of FSPs’ complaints-handling mechanisms, identifying anticompetitive practices, and monitoring suspicious transactions.

As such, market conduct supervisory authorities face significant and at times unique challenges. First, the type of data required to monitor compliance with market conduct regulation is often unstructured and can come from a wide range of sources. For example, in the case of financial consumer protection, a supervisory authority may analyze unstructured complaints data from the FSPs under its jurisdiction, relevant alternate dispute-resolution entities like financial ombudsmen (or a separate complaints-handling function within the authority), as well

4. *Unstructured data* refers to information that does not adhere to a predefined structure (for example, numeric or categorical). Text is a common example of unstructured data—for example, a customer’s description of his or her complaint against an FSP.

5. The term *artificial intelligence* is used broadly in this note and covers such subfields as machine learning and natural language processing.

6. For a broader discussion of artificial intelligence and machine learning in financial services, see FSB 2017.

as various media and social media sources. The unstructured nature of the data and diversity of data sources create challenges in data aggregation and analysis to identify potential risks to consumers and the market.

Second, the complexity of the analyses undertaken by market conduct supervisors is often due to its qualitative nature. For example, a market conduct supervisor may have to determine compliance with principles-based regulation, such as whether a certain business practice is “fair” to the customer. The result is that effective market conduct supervision relies heavily on professional judgment and the relationship between such judgment and data-driven analysis is not always straightforward. This aspect of market conduct supervision also raises the potential value of artificial intelligence applications to lighten the burden of supervisory authorities in efficiently filtering and analyzing such qualitative data, while maintaining control over supervisory judgments that are ultimately made.

Third, the proliferation of new Fintech market entrants and digital financial services adds further complexity to the supervisory process, as digital financial services models can be accompanied by new sources of consumer risk (for example, with respect to data privacy). This is particularly relevant in instances where a robust market conduct regulatory framework is not yet in place and supervisory author-

ities are pursuing a “test and learn,” or sandbox, approach to understanding consumer or market risks associated with a new provider, delivery channel, or product.

Finally, many market conduct supervisors operate in jurisdictions in which the regulatory or supervisory framework for market conduct is not fully developed. This can result in insufficient resources, limited staff capacity, and a lack of appropriate powers to undertake market conduct supervision.

How can Suptech support supervisory authorities in addressing these and other supervisory challenges? Potential use cases and outcomes include the following:

- **Automated data collection:** Suptech solutions can be deployed to improve the timeliness, scope, and granularity of collected data and to reduce reliance on manual processes. Data-input and data-pull systems are two Suptech solutions that relieve FSPs of the burden of data aggregation; instead, an FSP’s raw data is shared with the supervisory authority. Examples in Austria and Rwanda illustrate these approaches. (See box 1.)

Machine readable and executable regulation is another tool in which regulatory reporting requirements are coded into a language that can be read and executed by a machine. Supervisory authorities in the United

BOX 2.1

Automated Data Collection in Austria and Rwanda

Supervisory authorities in Austria and Rwanda have developed Suptech solutions for automated data collection that can be leveraged for market conduct. The Austrian example represents a data-input approach, while the Rwanda example represents a data-pull approach.

The Austrian central bank, in collaboration with Austrian banks, has developed an innovative data-input regulatory reporting platform that provides a direct interface between the IT systems of the central bank and banks. The platform allows banks to upload data in a standardized format, according to Austrian central bank requirements and specifications. The central bank can then transform the data into “smart cubes,” or data sets, containing specific data and information relevant for different departments within the Austrian central bank. This new model ensures more consistent and higher-quality data, relieves banks from having to prepare different reports for different supervisory

departments, and allows cost sharing of compliance between the supervisor and industry.

Another example is an automated data-pull system developed by the National Bank of Rwanda to enable supervisors to access raw data from supervised FSPs’ systems and then process the data into reports using its own software. The system comprises an electronic data warehouse to automate and streamline the reporting processes that inform and facilitate supervision. The data warehouse permits the National Bank of Rwanda to automatically “pull” data from the systems of supervised entities, reducing the need for manually produced reports and improving accuracy and consistency of data. The electronic data warehouse also facilitates daily automated data pulls for certain types of data. This approach does however generate new concerns and challenges, including those related to data privacy, operational risk, and reputational risk.

Kingdom are actively exploring this approach, as detailed in box 2.

Such automated data-collection tools can represent the intersection of Regtech and Suptech, as both the FSPs and the supervisory authorities are using the same technology. Automated data collection can yield a range of granular data, often in real time, create cost and temporal efficiencies for supervisory authorities, and free up staff resources from manual processes for tasks that require professional judgment. Automated data collection is an essential first step that can lead to material time and cost savings and improve supervisors' ability to monitor risks and trends. On the horizon are a number of other innovations being developed to improve the granularity, timeliness, and accuracy of data, allow more complex data analyses and risk assessments, and facilitate real-time supervision of the financial system.

- **Advanced data validation, analysis, and visualization:** Suptech solutions can be deployed to clean and analyze unstructured data, such as analysis of marketing materials or consumer agreements using natural language processing. Sentiment analysis can be used to analyze attitudes expressed in unstructured data

such as social media posts, customer reviews, or consumer complaints. Advanced analytical tools can be deployed to detect spikes and trends in key market conduct indicators—for example, to detect a rise in a certain type of potentially suspicious transactions. Such Suptech solutions can enable accurate and timely identification of risks to inform risk-based supervision, including for new Fintech market entrants and digital financial services.

- **Platform and database integration:** Integrated platforms can be useful tools for enabling data collection and validation between FSPs and supervisory authorities, equipping examiners with relevant information during on-site inspections, and facilitating the resolution of consumer complaints. Similarly, technology can be leveraged to merge disparate, often “noisy” data sets. As mentioned above, process automation can be leveraged to integrate a range of data (for example, monthly off-site supervision returns, financial ombudsman data, and credit bureau data) into a single platform or data set. These platforms and data sets can generate more efficient information flows across various stakeholders and ensure that supervisors have access to the full range of data and information needed for effective market conduct supervision.

BOX 2.2

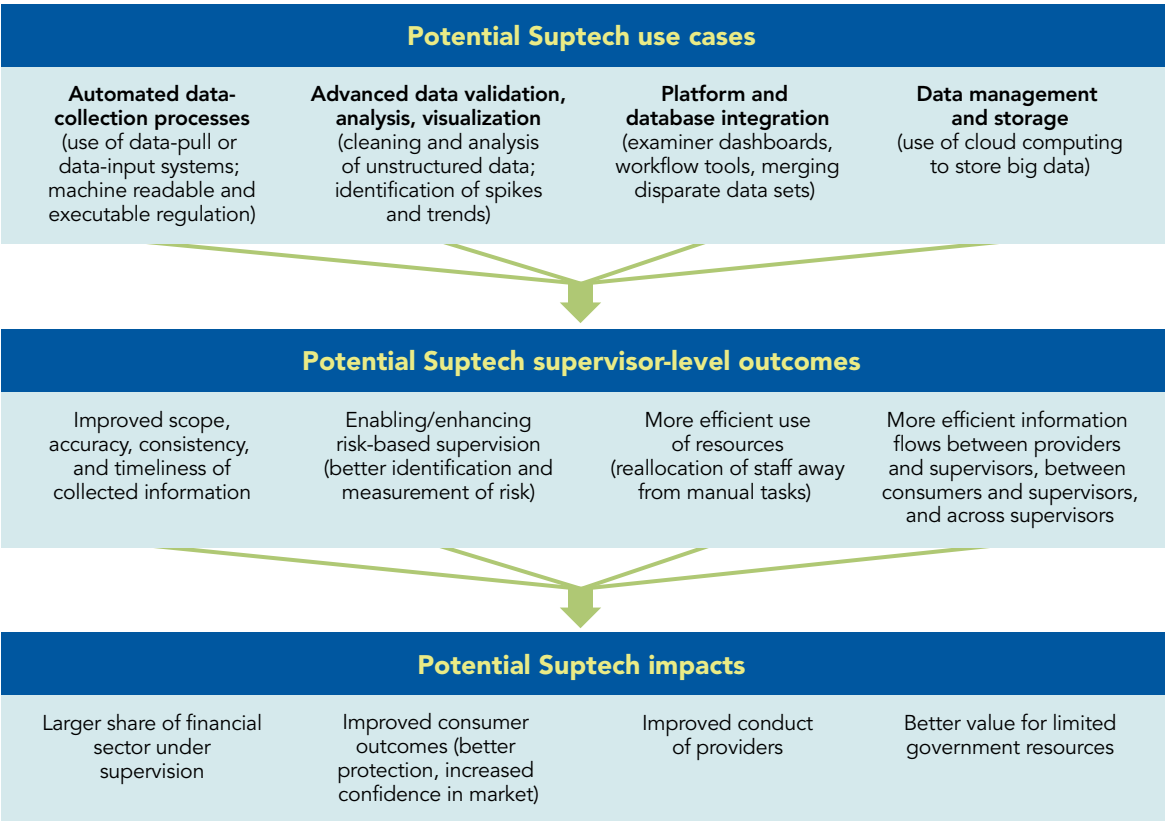
Exploring Machine Readable and Executable Regulations in the United Kingdom

The Financial Conduct Authority and Bank of England have begun exploring the potential for machine readable and executable regulations (MRERs), including through a TechSprint event hosted in November 2017. Creating an MRER means coding a regulatory requirement into language that can be read and executed by a machine. During the TechSprint event, participants successfully coded a small subset of reporting rules from the Financial Conduct Authority handbook into a language that machines can understand and execute by pulling the relevant information directly from the supervised entity. Participants also successfully simulated a rule change in the handbook in real time. The change was then automatically exe-

cuted by the supervised entity. In addition to temporal and cost efficiencies, MRER offers the potential to remove some level of ambiguity from the interpretation of regulatory rules and generate automatic reporting based on those rules.

As noted in a subsequent paper prepared by Immuta and the Yale Law School (Burt et al. 2017), MRER can be scaled either by focusing supervisory resources on validating MRER developed by supervised entities or by generating such code themselves. The paper also highlights a range of risks inherent in MRER, including incorrect interpretation, errors in the code base, lack of flexibility, and opportunities for abuse.

FIGURE 1: Suptech Conceptual Framework



- **Data management and storage:** Supervisory authorities must store efficiently and safely ever-increasing volumes of data. Cloud computing solutions can help to manage and store “big data,” enabling convenient on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage facilities, applications, and services) that can be rapidly released with minimal management effort or FSP interaction.

Figure 1 provides a conceptual overview of examples of Suptech use cases and potential outcomes for supervisors, along with potential overall impacts on supervisors, providers, and consumers.⁷

While Suptech solutions have the potential to improve the outcomes and impacts of supervisory activities, such enhancements are beneficial only to the extent that they facilitate a deeper understanding of risks, better decision making, and more efficient use of supervisory resources. Thus, a critical aspect of Suptech is the need to pair tech-

nology tools with a sound supervisory approach.⁸ The “Sup” and “Tech” components should form a feedback loop, where the appropriate supervisory approach drives the scope and form of Suptech solutions, and the technology helps to develop a more robust supervisory approach over time. These interactions are highlighted through the case examples in section 3.

3 SUPTECH IN PRACTICE: MARKET CONDUCT CASE STUDIES FROM THREE COUNTRIES

The Suptech case studies below describe technology solutions used by three supervisory authorities with different regulatory and supervisory structures, size and geographic spans of remit, and risks addressed. These include the U.S. Consumer Financial Protection Bureau (CFPB), the Bank of Lithuania, and the Central Bank of Brazil. It is worth noting that while the U.S. retail financial services

7. Other use cases, outcomes, and impacts are possible depending on the country context and specific applications of the technology solution.

8. As described in BCBS 2012, supervisory authorities should have a supervisory approach comprising a methodology for determining and assessing on an ongoing basis the nature, impact, and scope of risks, and processes in place to understand the risk profile of FSPs. See Core Principle 8.

market is much larger than that of Lithuania or Brazil, all three supervisors face similar supervision challenges, especially in that each supervisory authority's ambit covers far more FSPs than its staff can feasibly supervise on a consistent and active basis.

- Case studies 1 and 2 highlight the implementation of Suptech to enable the use of complaints data collection and analysis to enhance market conduct supervision, discussing technology implementations by regulators in the United States and Lithuania. The two supervisory authorities are at different stages of implementing and leveraging such technology, and the country examples are useful in both showing, and contrasting, their experiences and where they are heading. Although resolving consumer complaints and disputes is not a supervisory activity of itself, the collection and analysis of complaints data make up an important component of a comprehensive supervision program, such as for the purposes of generating indicators of heightened consumer risk.
- Case study 3 focuses on a Suptech solution created by the Central Bank of Brazil to facilitate remote market conduct supervision. Importantly, the development of the technology allows the central bank to supervise a large number of nonbank financial institutions, and provides a platform for expansion to other risk-based market conduct supervision activities, including consumer protection.

Each subsection below outlines both the Suptech solution and the supervisory approaches adopted, and how the the Suptech solution and the supervisory approach support and inform each other. The case studies also describe the implementation process taken by each supervisor and the outcomes, challenges, and lessons learned.

3.1 CASE STUDY: U.S. CONSUMER FINANCIAL PROTECTION BUREAU

Overview

The U.S. Consumer Financial Protection Bureau⁹ (CFPB) was established in 2011 as part of the package of post-financial crisis reforms contained in the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act. One of the primary mandates of the CFPB is to enforce consumer financial law consistently across depository and nondepository FSPs. With responsibility for insured depository institutions with total assets above \$10 billion and their

affiliates¹⁰ and tens of thousands of nonbank FSPs, the CFPB quickly identified a need for an effective, cost-efficient, and consistent way to identify and address consumer risks.

Technology solution

One of the CFPB's Suptech solutions to identify and address consumer risks begins with the use of a customer relationship management (CRM) system that serves as an online platform to facilitate the complaints-handling process between consumers and FSPs.¹¹ CRM systems are common in many industries (for example, sales, hospitality) and, in this case, provide financial consumers with a consistent user experience when submitting complaints and receiving responses across a number of FSPs.¹² The CRM is managed by the bureau's Office of Consumer Response (Consumer Response).

Consumers submit complaints via the CRM on the CFPB's website using complaint forms tailored to specific products. The consumer also submits a complaint narrative in which they describe the complaint or issue in their own words. The completed complaint forms generate structured data, while the complaint narrative represents unstructured data.

Although consumers can also submit responses by phone, mail, and so forth (CFPB staff members then input the submissions into the CRM manually), 81 percent of complaints in 2017 were submitted by consumers directly via the online CRM platform. Consumer Response manages these submissions along with those received from third parties (for example, from financial advisors, housing counselors, family members) and referrals from other agencies (such as state attorneys general).

Once a complaint is received, it is routed to the FSP via a secure company portal for response within 15 days. Most complaints (97 percent) receive FSP responses within the 15-day period (CFPB, "Submit a Complaint"). The FSP's response (if received) and basic information about the complaint (for example, the subject and date of the com-

9. The statutory name is the Bureau of Consumer Financial Protection, as per the Dodd-Frank Wall Street Reform and Consumer Protection Act.

10. CFPB 2017a presents a list of depository institutions subject to CFPB supervisory authority.

11. The CFPB defines *consumer complaints* as submissions that express dissatisfaction with, or communicate suspicion of wrongful conduct by, an identifiable entity related to a consumer's personal experience with a financial product or service. See CFPB 2017c, 60.

12. The CFPB does not directly resolve complaints or provide recommendations for their disposition. Rather, the bureau facilitates the process via the CRM and by encouraging FSPs to respond in a timely manner. The CFPB also does not verify all the facts alleged in these complaints, but it does take steps to confirm that a commercial relationship exists.

plaint) are published on the CFPB's public-facing Consumer Complaint Database (CCD). With the consumer's consent, the CFPB also publishes an anonymized version of the customer's complaint narrative.

An output of the CRM is the CCD, which contains real-time structured and unstructured data on consumer complaints sent to FSPs for response and FSP responses. The CCD provides financial sector stakeholders (including other financial sector regulators and state attorneys general) with a resource for identifying emerging trends in consumer risks.

A public version of the CCD is also posted to the CFPB's website and updated regularly. Aggregate complaints data can be downloaded as either a comma-separated value (.CSV) or Javascript Object Notation (JSON) file, or a subset can be downloaded (for example, all complaints for a specific product) by filtering the full data set and exporting the results. The public can also export the data using the CFPB's Open Data application programming interface (CFPB, "Consumer Complaints").

Interaction of technology solution with supervisory approach

The CFPB supervision function relies on analysis of available data about the activities of the entities it supervises, the markets in which they operate, and risks to consumers posed by activities in these markets. The real-time data in the CCD helps to trigger early warning systems and isolate trends by product, provider, or geographic area, enhancing the risk-focused nature of the CFPB's supervision planning and oversight.

Consumer complaints inform the following useful resources for the CFPB supervisors:

- **Customer Complaints Database:** Consumer complaints are available to a range of stakeholders in various forms. In addition to the public-facing CCD, there are internal versions that are used by supervision and enforcement teams to analyze the data for their own purposes, including as an input to the risk matrix that informs the annual examination schedule and for market monitoring reports.
- **Spikes and trends:** The "spikes and trends" tool is an advanced data analysis tool that flags short-, medium-, and long-term changes in complaint volumes in daily, weekly, and quarterly windows. Importantly, the tool works regardless of company size, random variation, general complaint growth, and seasonality. Reports based on the tool are distributed to a range of supervision and enforcement teams within the CFPB.

- **Company profiles:** Consumer Response produces company profiles that outline the complaint trends for specific FSPs. Such profiles include information on the issues complained about most frequently and trends over time. These are typically produced in advance of on-site examinations.
- **Company reports:** Consumer Response produces company reports that analyze the timeliness, accuracy, and completeness of an FSP's complaints response, as compared with its peer group.
- **Access portals:** The CRM also has several specialized portals to facilitate access by various internal and external stakeholders. There is a secure consumer portal, a secure company portal, a secure portal for other financial sector regulators (in the event that a complaint is outside the jurisdiction of the CFPB and needs to be forwarded to relevant authorities), and a secure portal for congressional offices.

The process to determine the annual examination schedule is an area where complaints data provides a critical resource.¹³ The CFPB's Reporting, Analytics, Monitoring, Prioritization and Scheduling Team is tasked with taking a data-driven and risk-based approach to developing the annual examination schedule. The CFPB's risk-assessment process focuses on specific product lines—known within the CFPB as institution product lines—rather than on the FSP itself, in order to foster a level playing field and consistent approach between nondepository institutions (which are often monoline) and depository institutions (which usually have multiple lines of business).¹⁴ The risk-assessment process is achieved through a supervision prioritization framework containing four inputs across the following two categories (CFPB 2013b):

Product markets

- **Market size:** the relative product market size in the overall consumer finance marketplace
- **Market risk:** the potential risk to a consumer from new or existing products offered in the market

Institution product lines

- **Institution product size:** an entity's market share or level of activity within a product market
- **Field and market intelligence (FMI):** other relevant information about a supervised entity

13. Institutions are not on a regular exam cycle.

14. This aligns with CFPB's objective of ensuring that consumer financial laws are enforced consistently across the market, without regard to business structure, type of charter, or location.

Complaints data is an important input into this process, along with a range of other resources.¹⁵ In particular, complaints data is a principal input into the quantitative component of the FMI risk score.¹⁶ The FMI captures potential consumer risks—including business, operational, and compliance—posed by an institution’s provision of services in a consumer market (excluding size). Complaints in a given institution product line are scaled for size and ranked by severity (high severity, medium severity, and low severity). A concentration of high-severity complaints is used as a proxy for higher risk in the quantitative FMI risk rating, which then is factored into the overall FMI risk rating and finally into the overall risk-tier rating.

Although the CFPB establishes an annual exam schedule, the process is dynamic. Supervisors are able to access real-time CCD data to help them respond to emerging risks as they appear throughout the year. For example, a spike in complaints for a given institution product line (as flagged by the “spikes and trends” tool and analyzed within a “spike and trend” memorandum) may result in the modification of the annual examination schedule or other forms of supervisory actions to include the relevant FSP.

Examiners are also able to access complaints data—including while on-site during an examination—via an internal online dashboard, which provides more dynamic and timely information than regular, static reports. The CFPB is in the process of integrating this dashboard with other tools used by examiners.

The “spike and trend” tool is also an effective early warning system that helps the CFPB to engage with companies outside the examination schedule structure. For example, in one instance, the examination team reviewed complaints associated with a spike in complaint volume and immediately reached out to the company to inform senior management and discuss consumers’ concerns. The CFPB was able to engage senior managers before they were aware of the matter through their own internal processes. The company quickly developed and implemented a plan to correct the issues, provided accurate information to customer service representatives, and developed a refund policy and process for affected con-

sumers, minimizing potential harm to consumers and further risk of exposure for the company (CFPB 2017b).

Complaints data are shared regularly with other regulators—including federal prudential regulators and state financial sector authorities—via a secure government portal. This secure portal includes more information than the public-facing website. The CFPB does not create regular, customized reports for different regulators, but it does respond to ad hoc requests from regulators and other government institutions, generally within two days.

The CFPB’s Office of Enforcement draws from complaints data as well as market monitoring, supervision, and external sources, such as other federal and state regulators and consumer groups, to identify which cases to pursue. This process is reactive based on evidence of consumer harm. Cases are selected based on the egregiousness of the case, number of customers harmed, and resources available to pursue. Enforcement staff members are able to access the complaints data and conduct their own searches and to share reports with other divisions and regulators, such as the U.S. Federal Trade Commission.¹⁷

The CFPB publishes a number of analyses on the complaints data. For example, a monthly complaints report summarizes complaints data trends by product, state, and company.¹⁸ The report also typically includes a “product spotlight” (for example, debt collection) and a “geographic spotlight” (such as Florida). The CFPB publishes the annual *Consumer Response Annual Report*, which summarizes consumer complaints by product.¹⁹ Finally, the CFPB reports semiannually to Congress and the president; the report typically includes an analysis of complaints data.²⁰

Implementation process

As a new organization, the CFPB’s Office of Consumer Response looked to the experiences of other regulators to understand the types of complaints to expect, and it used available complaints data to inform its phased roll-out of complaints handling by product (CFPB 2013a).

The CRM was initially developed by an external vendor, following an internal conceptualization by the CFPB. The

15. In addition to drawing from complaint statistics, supervision staff members synthesize information from a wide range of other internal and external sources, including (i) directly from the institution and through monitoring and examination activities; (ii) various CFPB market research, policy, consumer response, education, and subject matter (for example, Fair Lending) offices and divisions; and (iii) other state and federal regulatory agencies.

16. There is also a qualitative component.

17. The U.S. Federal Trade Commission (www.ftc.gov) also has enforcement authority for certain consumer financial products sold by nonbanks and functions similarly in a reactive enforcement mode based on complaints and referrals. The CFPB and FTC share enforcement responsibility for a few products under a memorandum of understanding (Memorandum 2012).

18. See example at CFPB 2016.

19. See example at CFPB 2018.

20. See example at CFPB 2015.

CRM was developed and launched under intense time pressure in less than 60 days. More recently, the CRM has been migrated to another system in order to integrate with the broader IT system of the CFPB.

The CFPB phased in its complaints handling for the products and services under its authority gradually over time: credit card and mortgage complaints in 2011; bank accounts and services, private student loans, consumer loans, and credit reporting in 2012; money transfers, debt collection, and payday loans in 2013; prepaid cards, credit repair, debt settlement, pawn and title loans, and virtual currency in 2014; and federal student loan servicing in 2016. As of July 20, 2017, the CFPB has handled approximately 1.2 million complaints (CFPB website).

Outcomes, challenges, and lessons learned

The scope and quality of the CFPB's supervisory approach has benefited as a result of its Suptech-supported approach to complaints data capture and analysis. The CRM provides an innovative platform to collect nearly real-time data on consumer risks, which is used to inform risk-based supervision and enforcement activities. Internal tools (for example, dashboards) have also improved the flow of information within the CFPB and create an effective platform to facilitate the complaints-handling process between consumers and FSPs, which is an important element of financial consumer protection.

An ongoing challenge common to any jurisdiction with multiple regulators is enabling timely and accurate information sharing between different agencies. Memoranda of understanding establish a common understanding and process, but better technology interfaces, such as application programming interfaces, improve this flow. Sharing information between different regulators raises customer and FSP privacy and confidentiality issues under U.S. regulations, however, so a balance needs to be achieved.

Many countries lack the resources available to the CFPB, but this does not preclude development of a basic yet robust system in a smaller country. Case study 2 explores a more streamlined yet effective approach to leveraging complaints data to inform market conduct supervision.

3.2 CASE STUDY: BANK OF LITHUANIA

Overview

The Bank of Lithuania (BoL) supervises close to 500 FSPs and has a mandate to undertake both prudential supervision and market conduct supervision (BoL 2017b). The

Law on Consumer Protection further provides BoL with the authority to handle complaints as well as settle disputes between consumers and FSPs.²¹ To support these mandates, in 2016 BoL introduced an electronic system to enhance its complaints-handling and dispute-resolution activities and to capture complaints data more effectively for incorporation in its supervisory work. Prior to the introduction of this system, all consumer submissions were communicated via post, by e-mail, or in person at the BoL. Information relating to the complaints and disputes was then captured and analyzed largely through an onerous manual process. This made it difficult to keep track of dispute-resolution deadlines and decisions and, relevant for the discussion here, limited the timeliness and usefulness of such data for supervisory activities.

BoL's recently introduced electronic system now enables consumers to submit complaints and disputes online and allows BoL to store and track progress on the submissions within a single database. Importantly, the data captured by the electronic system is incorporated into BoL's supervisory risk assessments, at both the provider and the market level. Although the system is still in the early stages of implementation, it has already begun to improve the efficiency and effectiveness of BoL's supervisory processes. For example, it informed a recent decision to undertake a thematic review of a particular product category.

Technology solution

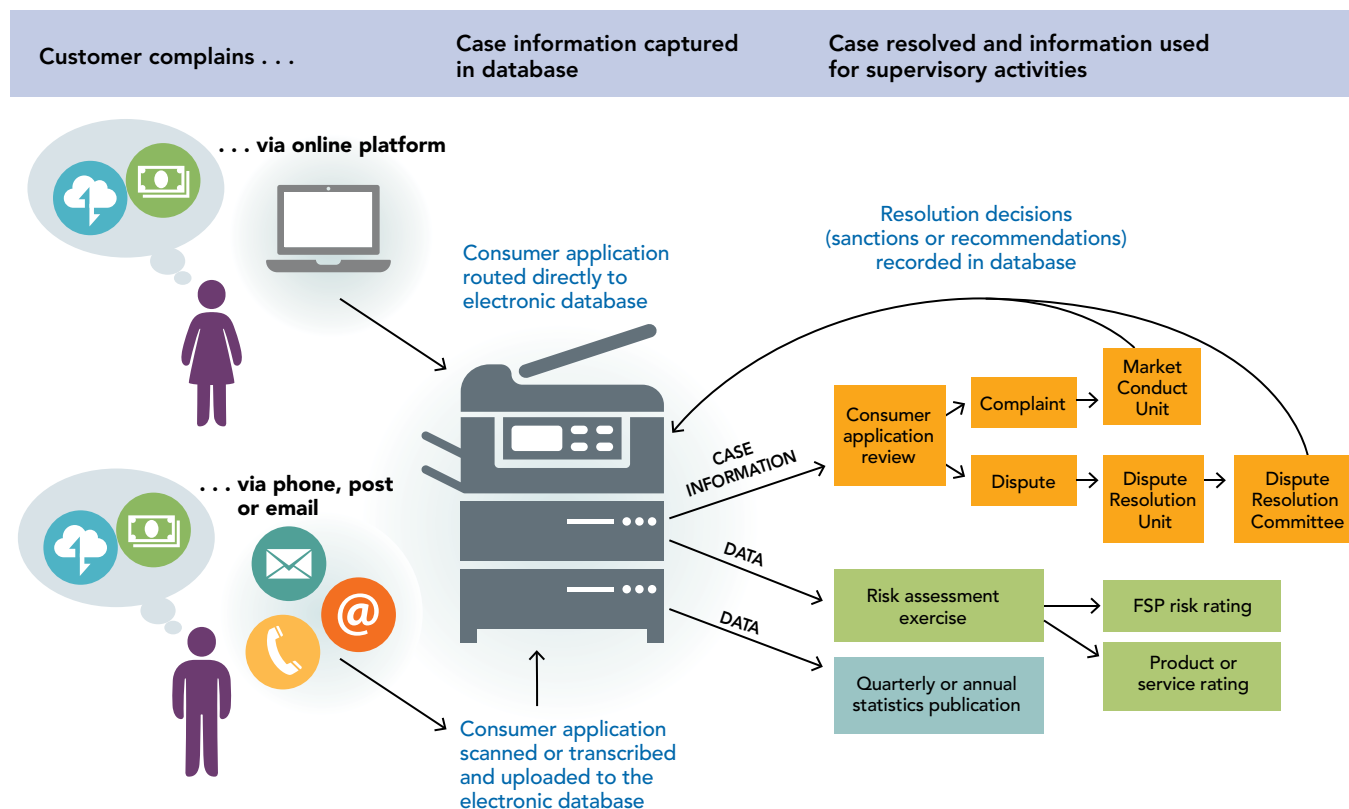
The electronic system is made up of two components: an online complaints and disputes submission platform hosted on BoL's website, and an internal electronic database that stores relevant documents and decisions relating to a case. (See figure 2 for an illustration of the system.) The online submission platform allows consumers to lodge a complaint or dispute application directly through BoL's website using an electronic signature (BoL 2017a).

Once a consumer's application has been submitted via the online platform, it is automatically matched to the relevant FSP's record in the internal database.²² Complaints and disputes that are not submitted online (those that are submitted, for example, via e-mail or through the post) are scanned and manually uploaded into the internal database. The consumer complaint or dispute application is then assessed by staff in the Financial Services and Markets Supervision Department to determine whether it

21. *Complaints* are considered to be violations of consumer rights related to noncompliance with laws and regulations applying to FSPs. *Disputes* are defined as breaches of contractual obligations between consumers and FSPs.

22. The internal database also stores all other relevant information relating to an FSP, including licenses.

FIGURE 2: Bank of Lithuania's Electronic Complaints System



relates to a complaint or a dispute, and the case is then routed to either the dispute-resolution unit or the complaints-handling unit.

Data and findings resulting from complaint investigations are sent to the heads of divisions within the Financial Services and Markets Supervision Department. This data is then used to determine whether an inspection should be conducted or other administrative sanctions should be applied to a particular FSP. For dispute investigations, findings are submitted to the Dispute Resolution Committee—comprising members from five different divisions within BoL—which issues nonbinding recommendations to consumers and FSPs. All activities and decisions relating to the complaint or dispute are stored in the internal database.

The database then allows the generation of risk profile reports for specific FSPs. The reports are made available to supervision department staff not only on an annual basis for FSPs judged of most significance, but also on request for other FSPs. Complaints data is analyzed to identify weaknesses and risks arising from FSPs' activities and processes, including at individual stages of the product life cycle, such as product oversight and governance, product sales, information disclosure, and so on.

BoL expects that increasing the amount of qualitative data captured through the system allows it to better assess both FSPs' regulatory compliance and how fairly they treat their consumers.

Interaction of technology solution with supervisory approach

BoL has adopted a risk-based approach to market conduct supervision—that is, resources are allocated toward more significant financial market participants or toward financial services and products posing the highest risk to consumers (BoL 2017b). An annual risk-assessment exercise is carried out to plan for on-site inspections of FSPs, as well as for thematic reviews of particular financial services and product types. However, inspections can be accelerated during the year when there are indications of increased risk, including risks to consumers.

As part of its risk-assessment exercise for FSPs, BoL has created a risk matrix that categorizes FSPs into four categories based on a number of indicators, including the institution's size, systemic importance, uniqueness, and other quantitative and qualitative indicators. While this exercise covers mainly traditional prudential risks, BoL

FIGURE 3: Scope of Risk-Assessment Exercise for FSPs

Source: Bank of Lithuania

is increasingly using data generated by the electronic database—for example, the number of complaints levied against an FSP—to inform the risk rating of FSPs from a market conduct perspective. (See figure 3 for the range of risks considered.)

For BoL's risk assessment of financial services and product types from a market perspective, the bank relies almost entirely on statistics from the electronic database. This risk assessment does not necessarily take into account the size or systemic importance of FSPs; rather, it focuses on the risks posed to consumers based on the complaints levied against particular financial products. Once a high-risk financial service or product type is selected, on-site inspections are then carried out across providers of the selected financial products, regardless of the size of the institution.

Outcomes, challenges, and lessons learned

BoL made the decision to develop the electronic complaints and disputes system as part of a broader internal strategy to minimize the number of platforms and to integrate different systems within BoL better. After weighing the option of purchasing an off-the-shelf system versus developing the system in-house, BoL determined that the in-house option would better achieve their overall objectives. The system was developed over 10 months by BoL staff and is based on an Oracle database and the Microsoft SharePoint system.

From a supervisory perspective, BoL has identified benefits resulting from use of the recently implemented system. They include more granular analyses and speedier completion of such analyses. However, work on enhancing the electronic database and the tools it supports is ongoing.

For example, BoL is planning to incorporate additional analytical tools in the system to enable the supervision teams to engage better with the data stored in the database for their supervisory activities.

BoL is also working to modify the system to allow consumers and FSPs to track progress of their complaint and dispute cases.²³ While the electronic system has enabled BoL to increase the efficiency of its consumer complaints and dispute-resolution processes, only 25 percent of complaints and disputes are currently submitted online. BoL is thus working to increase awareness of the online submission platform, and it is hoped that greater use of the online submission platform will be encouraged by proposed upgrades to the system that will enable consumers and FSPs to track progress of their cases directly.

While BoL's technology implementation is ongoing, its experience shows that by building on existing technology, supervisory authorities can begin to generate useful data and information that can assist in identifying and responding to consumer risks in a timely manner while better managing staff and other supervisory resources.

3.3 CASE STUDY: CENTRAL BANK OF BRAZIL

Overview

In 2011, the Central Bank of Brazil (BCB) identified a need to develop and implement a risk-based AML/CFT supervision approach for the Brazilian bank and nonbank financial institution (NBFI) sector.²⁴ This was due to a number of internal and external drivers, including recognition of the need to capture the risks in this sector better to ensure a sound and safe national financial system, and to align more closely with international recommendations and best practices. However, a key challenge facing BCB was the limited resources to oversee the large number of banks and NBFIs (more than 1,600), which were heterogeneous and located over a vast geographical area. BCB therefore recognized that its supervision program would require enhanced technology paired with a sound risk-based methodology to accomplish its goals.

23. Communication to consumers and FSPs is currently done through stated preferred channels—that is, by e-mail or via the post.

24. In the Brazilian context, NBFIs include credit and deposit-taking financial institutions, such as consumer finance institutions, securities and exchange brokerage institutions, security distribution institutions, leasing companies, microfinance institutions, development agencies, mortgage companies, payment institutions, and credit unions.

Technology solution

BCB's Integrated System for Supervision Support and Communication (SisCom) is a web-based system that allows easy and secure sharing of information. It is a communication platform that supports a process for collecting data and documents through a web portal and for interacting online with even hard-to-reach FSPs in a cost-effective way; it also enables inspectors to carry out remote supervision. The data collected is mostly qualitative (for example, FSPs' governance, systems, and controls to mitigate the AML/CFT risks), but it can also be quantitative as relevant to assess risks and controls. The information is collected using questionnaires and forms developed by supervisors to collect detailed information and uploaded documents, according to the supervisory activity that has been planned. (Figure 4 shows levels/tiers of risk-based inspections.)

SisCom does not analyze or validate all data submitted by banks and NBFIs automatically, although part of the information is validated by the supervisors using other internal and external systems. Besides collecting data, the system facilitates the full supervisory process, such as creating formal letters and information requests that are automatically sent to FSPs²⁵ and managing the follow-up process by the

FSP. Final supervision reports are generated automatically, using all the information that was input into the system. These functions have increased the transparency, consistency, and efficiency of the supervision process.

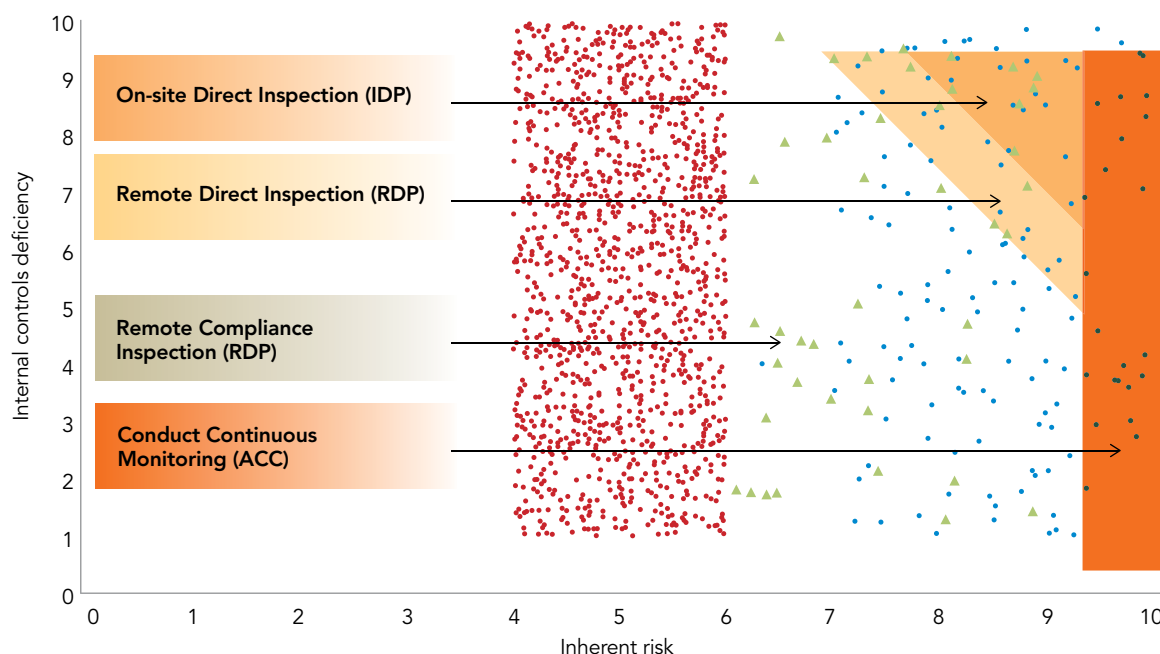
The system also allows forms to be customized and standardized, such as information requests to be sent to FSPs as part of the supervision and examination procedures followed by inspectors. For example, a preloaded form tailored to a specific NBFIs sector and topic, such as an AML/CFT review of a foreign exchange broker, could be automatically sent by the system. Each individual NBFIs completes and uploads the forms within a certain number of days as specified by BCB.

Interaction of technology solution with supervisory approach

The data collected by SisCom feeds into a methodology that allows BCB to segment and supervise banks and NBFIs by different risk categories. Inspectors use the system to record the analysis, documentation, and conclusions. The quantitative and qualitative data are processed and analyzed by the supervisors to provide them with two different perspectives: (i) level of compliance with specific regulatory requirements, and (ii) risk assessment, using a rating categorization, based on the risk-based methodology. In case the provider needs further documents and clarifications, the system provides the supervision team with a "chat box" tool to interact easily and quickly with the FSP (available for any type of inspection).

25. Standardized, formal letters and information requests are manually created by supervisors in the system and are then automatically replicated and sent to all FSPs, increasing efficiency in the supervisory process.

FIGURE 4: Central Bank of Brazil's Conduct Risk Framework for NBFIs



BCB defines four levels or tiers of risk-based inspection (see figure 4), and it is possible to use SisCom to collect the following data for any inspection tier, as needed.

1. Remote compliance inspection: All low and medium AML/CFT-risk banks and NBFIs undergo this basic remote inspection, which provides an initial overall risk appraisal based on compliance risk and controls for each element.
2. Remote direct inspection: A more focused, in-depth remote inspection, this type of inspection aims at covering specific issues in more detail, depending on the initial risk assessment. It would still be undertaken remotely, using the system to collect and structure the information. For this purpose, specific information requests and examination forms would be appropriately tailored.
3. On-site direct inspection: This inspection includes some remote aspects but will be undertaken mainly on-site, generally in cases in which the perceived risk is higher.
4. Continuous monitoring: This in-depth on-site inspection covers the most relevant banks in terms of money-laundering risk (among which are systemically important financial institutions) by continuously assessing corporate governance, risk management, and compliance.

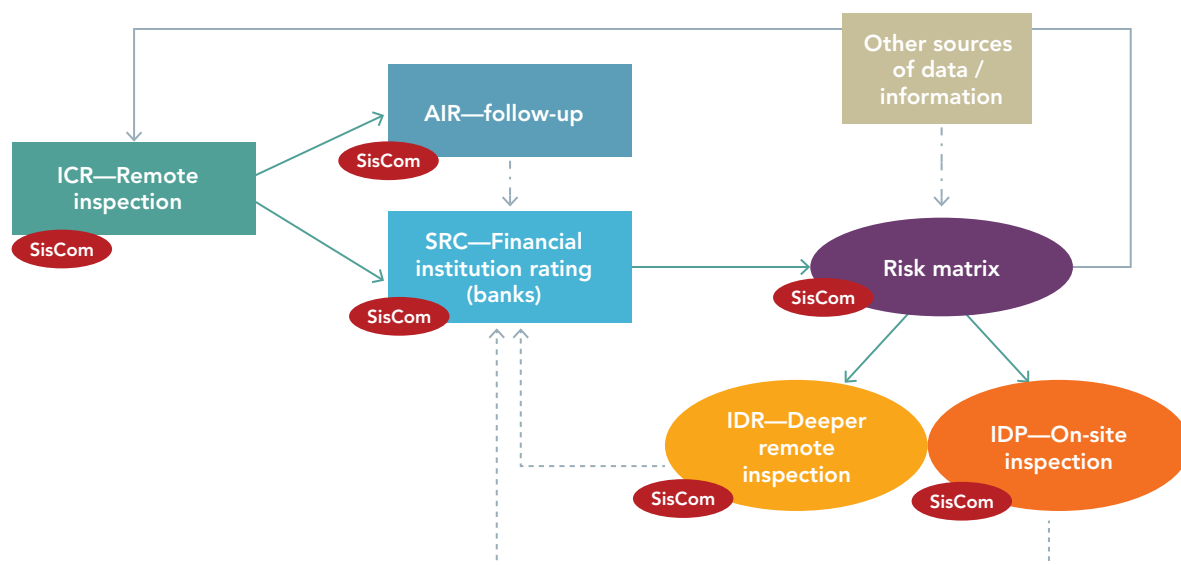
Figure 5 shows the workflow, based on the tiers of risk-based inspection and the use of SisCom at each step. Internal control deficiencies are assessed during the remote compliance inspection, in which inspectors apply risk assessment parameters and use the system to attribute ratings to each control element by FSP.²⁶ Ratings range from 1 to 4, with a rating of 1 indicating good internal controls and 4 for very deficient internal controls. The inherent risk is assessed in the risk matrix (figure 4), using the same rating system, in which 1 is low and 4 is high inherent risk. A combination of high inherent risk and high deficiencies in internal controls would plot the FSP in the red area of the graph shown in figure 4, indicating the need for increased supervisory attention, including for on-site inspections.

Implementation process

While the need for technology to support the aims and activities outlined above was clear, BCB had to decide whether such technology should be acquired from a vendor or developed in-house. Based on previous experience, BCB decided the best approach would be to develop the software in-house. Key factors on which this decision was based included the lengthy lead time (estimated at 10 months) that would be required to contract for a project of this size and scope, the difficulty in finding an existing product that met their specifications, and the

26. BCB reports that the automation of the risk assessment, using the system to attribute rates, is to be developed.

FIGURE 5: Central Bank of Brazil's Conduct Inspection Workflow for NBFIs



Source: Central Bank of Brazil

fact that BCB had capacity to do so. Designing and developing the software in-house offered substantial cost savings and allowed for customization, permitting the system to be aligned with the supervisory methodology also in development in parallel with the system.

The development process was a close collaborative effort between the IT and supervision departments, requiring a commitment of six staff members and more than two years' time for the design, development, and initial implementation. The close involvement of supervision staff in the design of the system resulted in a fairly smooth implementation process. BCB conducted training for external users at the beginning of each round of supervision, by bank and NBFI sector. The new supervisory approach and how to use the system was explained, keeping in mind that different users have different access levels, according to their profiles in the system. For example, the FSP's internal audit department accesses different forms than compliance officers. Additionally, a help desk was created to provide clarification and technological assistance tailored to the different financial industry sectors, some comprising over 100 providers.

Outcomes, challenges, and lessons learned

SisCom was considered a successful solution to BCB's challenge of launching a new supervisory program for a large and unfamiliar sector with diverse risk profiles. By using technology to improve data collection and communication, BCB was able to allocate scarce supervisory resources more appropriately where risks are elevated. The operational needs of a sound underlying methodology were respected during development of the technology, allowing for a process that provides a systematic and transparent means of fulfilling the AML/CFT oversight mandate.

Given the successful experience with AML/CFT, supervisors responsible for consumer protection and other BCB supervision departments started implementing SisCom to increase efficiency in their supervisory processes. This was possible because the system was developed to be flexible and customizable.

A key challenge related to the fact that the technology solution was designed in parallel with the development of a new supervisory approach and workflow process, rather than to support an existing process. This resulted in a prolonged test-and-learn process in which both the technology solution and the workflow process were being jointly developed and revised.

Another challenge was a low level of technological capacity at some of the FSPs. So an important consideration is

infrastructure of the country and FSP readiness for such a system, as well as a phased implementation process.

At the beginning of 2018, BCB began migrating SisCom to a new platform, the Automated Supervision Process (APS), which unifies the various supervision applications used by BCB and integrates them with other systems within BCB. The aim of the APS project has been to (i) provide a unified view of supervisory information, (ii) improve the sharing of information, (iii) ensure the security of information, (iv) streamline and increase the productivity of the supervisory process, (v) enhance the management of the supervisory team and activities, and (vi) lower compliance costs to FSPs. It is expected that by the end of 2018 all communications with FSPs will be undertaken using the APS and that the majority of inspections and follow-up activities will be managed through the APS.

4 CROSS-CUTTING CONSIDERATIONS

The case studies outlined in section 3 highlight how Suptech solutions can be leveraged to improve market conduct supervision processes in different jurisdictions. In particular, the case studies illustrate that Suptech use cases and outcomes are possible regardless of the size or maturity of the jurisdiction.

While both the CFPB and BoL use technology to leverage the collection, validation, analysis, sharing, and dissemination of complaints data, they have, importantly, focused the development of their technology solutions on informing and enhancing supervisory approaches, rather than designing the supervisory approach around the technology tool (which could result in a less effective response to relevant risks and the supervisory context).

These advances within the CFPB and BoL have improved the quality, consistency, and timeliness of complaints data, expanded the scope of data-collection efforts to meet an evolving mandate, more efficiently allocated staff resources, and improved the flow of information between FSPs, consumers, and supervisors and (in the case of the CFPB's Open Data application programming interface) allowed for more widespread dissemination of data in the financial sector.

BCB's case similarly highlights a use of Suptech that has resulted in improved data collection in a cost-effective way, and better analysis of risks and trends based on that data. Since its launch, the technology platform has achieved a number of important outcomes: improved quality, consistency, and timeliness of data, expanded

scope of data collection, more efficient allocation of staff resources, and better flow of information between FSPs and supervisors. BCB has consequently been able to increase the share of the financial sector it has supervised in a cost-effective, risk-focused manner.

In developing and implementing supervisory approaches supported by Suptech, supervisory authorities will need to take into account a range of novel or changed considerations and risks, resulting from factors such as digital data collection and analysis, and automation of procedures. Some of the most critical are discussed below, which also include forward-looking considerations not explicitly addressed in the case studies.

Technology as a Tool rather than a Supervisory Approach

Suptech solutions for market conduct supervision are most effective when designed as a tool to enable a well-developed supervisory approach. While supervisory authorities should leverage the opportunities provided by technology to improve supervisory approaches and processes, the parameters of the Suptech solution should not be the key determinant of the supervisory approach. In short, supervisory authorities should not settle for being passive adopters of tools and solutions designed by external vendors or internal IT staff. Rather, as far as practicable, supervisory authorities should push for technology solutions to be tailored to their supervisory and organizational needs. Thus, in developing and refining their supervisory approaches, supervisory authorities should work toward identifying functional requirements and nonnegotiable outcomes for any technological solutions that are to support those activities.

For example, in interviews conducted for the purposes of this note, several technology service providers indicated that it would be possible to adapt their technology solutions for market conduct supervision purposes. However, a constraint to developing such off-the-shelf products remains the lack of consensus (both within individual jurisdictions and globally) on appropriate metrics or indicators for market conduct supervision. This suggests that in many jurisdictions, more work may be needed to develop a supervisory approach for market conduct before necessarily seeking a Suptech solution that is automatically able to implement it. One ongoing initiative in this area is the work being done by the Organisation for Economic Co-operation and Development Task Force on Financial Consumer Protection to develop a risk dashboard of possible indicators to monitor consumer protection risks. (See OECD 2018.)

Capacity of Supervisors

An important consideration when acquiring or developing Suptech solutions is the readiness of supervisors at every level of the organization to be able to use and administer such technology. Defining initial business workflow and data needs, pilot testing new software, conducting initial and ongoing training, and fostering a positive culture of innovation should be encouraged so that management and staff understand and benefit from technology enhancements while appreciating the new risks and demands that come with it. Top-level managers do not need to understand programming and other technical aspects of a proposed Suptech solution, but they should have sufficient knowledge of the outcomes of such solutions in order to make sound decisions regarding purchases, customization, and upgrades. This is important to ensure that Suptech investments are appropriate to the needs and resources of the supervisory authority. Supervisors may want to consider developing a formal technology strategy to ensure that the proper systems are in place and that staff skills are sufficient to implement and manage new technologies.

Another key area is the capacity of the supervisor to shift from compliance-based supervision to risk-based supervision, a shift that can be enabled by Suptech solutions. Risk-based supervision typically requires greater application of professional judgment. For instance, Suptech solutions may provide new data or new analytical tools to inform a risk rating, but professional judgment is critical to validate and, in some cases, modify the risk rating (often within certain constraints). Professional judgment is also necessary to determine the thresholds and analytical approaches to determine the risk rating in the first place. In such cases, it may be necessary to build the capacity of supervisory staff or to recruit staff with the requisite skills.

Finally, in leveraging Suptech solutions for advanced data analysis, supervisory authorities need sufficient capacity to develop and refine the models onto which the Suptech solution is deployed—for example, defining the question, determining the measurement approach, generating the appropriate data, and assessing the model's accuracy.

Capacity of FSPs

Supervisory authorities will also need to assess FSPs' capacity to adopt new technologies and interact with the Suptech solutions being implemented by the supervisory authority. Significant lead time and training may be necessary for less sophisticated FSPs to upgrade their systems and staff skills and implement proper audit and controls so that data and reports are accurate and subject to adequate protections. In instances where a single technology

solution is used by both the supervisor and the FSP, discussions on appropriate levels of cost sharing may also be necessary. Finally, in instances where an FSP has a higher level of technological sophistication than the supervisory authority, consideration should be given to the risk that the FSP may be able to use the technology or capacity gap facing the supervisory authority to its own advantage, and to measures to be taken to mitigate such risks.

Operational Risk Management and Data Security

At a broader level, policy makers will continuously need to assess the effect of technology on data security and privacy so that an appropriate balance between innovation, efficiency, and data protection is maintained. Data protection and privacy laws should be flexible enough to facilitate innovative new ways of accessing data for supervisory purposes while protecting the privacy and security of this data. Strong operational risk management and controls

will be critical for supervisors who have greater access to FSP data as part of monitoring and reporting processes, such as in the data-pull and data-input approaches. Supervisors should clearly define and follow secure access protocols to avoid placing customer and FSP data at risk, and use strong firewalls and systems to prevent unauthorized access through external hacks or internal misuse. Supervisors should carefully weigh decisions related to expanding access to data, so that privacy and security risks are proportional to the value of fulfilling the supervisory mandate.

Supervisors should also identify and address operational, reputational, and liability risks inherent in greater access to data. For example, a supervisory authority that gains real-time access to granular data of an FSP may be seen as increasing its responsibility for not addressing misconduct that could have been predicted from the data.



REFERENCES

- BCB (Central Bank of Brazil) (website), <http://www.bcb.gov.br>.
- BCBS (Basel Committee on Banking Supervision). 2012. *Core Principles for Effective Banking Supervision*. Washington, DC: Bank for International Settlements. <https://www.bis.org/publ/bcb230.pdf>.
- . 2017. *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors*. Washington, DC: Bank for International Settlements. <https://www.bis.org/bcb/publ/d415.pdf>.
- BoL (Bank of Lithuania) (website), <https://www.lb.lt/en/>.
- . 2017a. “Settle a Dispute with a Financial Service Provider” (web page), <https://www.lb.lt/en/dbc-settle-a-dispute-with-a-financial-service-provider>.
- . 2017b. “Supervisory Activities” (web page), <https://www.lb.lt/en/supervisory-activities>.
- Burt, Andrew, Jeremy Aron-Dine, Eugene Kim, Catherine Martinez, and Xiangnong (George) Wang. 2017. “2017 Model Driven and Machine Executable Regulations Tech Sprint: Successful Criteria and Recommendations.” College Park, MD: Immuta, and New Haven, CT: Information Society Project, Yale Law School. <https://www.immuta.com/download/recommendations-for-the-fca-and-boes-2017-model-driven-and-machine-executable-regulations-tech-sprint/>.
- CFPB (Consumer Financial Protection Bureau) (website), <https://www.consumerfinance.gov/>.
- . n.d. “Consumer Complaints” (web page), <https://dev.socrata.com/foundry/data.consumerfinance.gov/jhqv-w97w>.
- . n.d. “Submit a Complaint” (web page), <https://www.consumerfinance.gov/complaint/>.
- . 2013a. *Consumer Financial Protection Bureau Strategic Plan, FY 2013–FY 2017*. Washington, DC: CFPB. <http://files.consumerfinance.gov/f/strategic-plan.pdf>.
- . 2013b. *Supervisory Highlights*. Summer 2013. Washington, DC: CFPB. https://files.consumerfinance.gov/f/201308_cfpb_supervisory-highlights_august.pdf.
- . 2015. *Semi-Annual Report of the Consumer Financial Protection Bureau, April 1, 2015–September 30, 2015*. Washington, DC: CFPB. http://files.consumerfinance.gov/f/201511_cfpb_semi-annual-report-fall-2015.pdf.
- . 2016. *Monthly Complaint Report*. Vol. 9 (March 2016). Washington, DC: CFPB. <https://www.consumerfinance.gov/data-research/research-reports/monthly-complaint-report-vol-9>.
- . 2017a. “Institutions Subject to CFPB Supervisory Authority” (web page), <https://www.consumerfinance.gov/policy-compliance/guidance/supervision-examinations/institutions/>.

- . 2017b. *Supervisory Highlights*. Issue 15 (spring 2017). Washington, DC: CFPB. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201704_cfpb_Supervisory-Highlights_Issue-15.pdf.
- . 2017c. *Monthly Complaint Report*. Vol. 24 (June 2017). http://files.consumerfinance.gov/f/documents/201706_cfpb-Monthly-Complaint-Report-50-State.pdf.
- . 2018. *Consumer Response Annual Report, January 1–December 31, 2017*. Washington, DC: CFPB. https://www.consumerfinance.gov/documents/6406/cfpb_consumer-response-annual-report_2017.pdf.
- FCA (Financial Conduct Authority). 2017. “RegTech” (web page), <https://www.fca.org.uk/firms/regtech>.
- Fernández Espinosa, Luz. 2016. “10 Keys to Understand What Regtech Is All About.” BBVA (Banco Bilbao Vizcaya Argentaria) blog, May 23, 2016. <https://www.bbva.com/en/10-keys-understand-regtech/>.
- FSB (Financial Stability Board). 2017. *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities’ Attention*. Basel, Switzerland: FSB. <http://www.fsb.org/wp-content/uploads/R270617.pdf>.
- IIF (Institute of International Finance). 2016. *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*. Washington, DC: IIF. <https://www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting>.
- IRTA (International Regtech Association). n.d. “Supporting the Development and Adoption of Regtech.” IRTA blog, <https://Regtechassociation.org/2017/04/20/supporting-the-development-and-adoption-of-Regtech/>.
- Memorandum of Understanding between the Consumer Financial Protection Bureau and the Federal Trade Commission, January 20, 2012. <https://www.ftc.gov/system/files/120123ftc-cfpb-mou.pdf>.
- OECD (Organisation for Economic Co-operation and Development). 2018. *Financial Consumer Protection Risk Drivers: A Framework for Identification and Mitigation in Line with the High-Level Principles on Financial Consumer Protection*. DAF/CMF/FCP/RD(2017)3/FINAL. Paris, France: OECD. [https://one.oecd.org/document/DAF/CMF/FCP/RD\(2017\)3/FINAL/en/pdf](https://one.oecd.org/document/DAF/CMF/FCP/RD(2017)3/FINAL/en/pdf).
- Petrasic, Kevin, Benjamin Saul, and Helen Lee. 2016. “Regtech Rising: Automating Regulation for Financial Institutions.” *White & Case*, September 26, 2016, <https://www.whitecase.com/sites/whitecase/files/files/download/publications/Regtech-thought-leadership.pdf>.
- Toronto Centre. 2017. “FinTech, Regtech and Suptech: What They Mean for Financial Supervision.” Toronto, Ontario: Toronto Centre. <http://res.torontocentre.org/guidedocs/FinTech%20RegTech%20and%20SupTech%20-%20What%20They%20Mean%20for%20Financial%20Supervision.pdf>.
- Woolard, Christopher. 2017. “The FCA’s Regional FinTech Engagement.” Speech delivered at Leeds Digital Festival, April 26, 2017. <https://www.fca.org.uk/news/speeches/fca-regional-fintech-engagement>.

