Institute of International Finance

MARCH 2016

REGTECH IN FINANCIAL SERVICES: TECHNOLOGY SOLUTIONS FOR COMPLIANCE AND REPORTING

INTRODUCTION

The financial services industry is seeing a flurry of innovation and increased competition due to the application of new technology in the sector. Financial institutions (FIs) are applying new technologies such as cloud computing, blockchain, machine learning, APIs and innovations in cryptography to reduce costs and friction, enhance security and enable new products and services.

The Institute of International Finance (IIF) and its Members see a great opportunity to apply these innovations to regulatory and compliance challenges as well. "Regtech," which we define as "the use of new technologies to solve regulatory and compliance requirements more effectively and efficiently" has enormous potential to enable better compliance solutions, increasing efficiency, profitability and reducing barriers to entry to the sector.[1] This is particularly promising in a sector with rapidly growing compliance costs, in which an uncertain macroeconomic and financial environment is putting pressure on the sector's profitability.

This report analyzes how new technology can be applied to improve compliance and regulatory reporting. It identifies areas in compliance that could benefit from regtech, describes recent technological innovations and how they could be applied to compliance and reporting, and discusses barriers to regtech implementation and development. FIs have a primary responsibility for supporting regtech development, most importantly by creating IT and risk infrastructures that are capable of integrating these new solutions.

"FIs have a primary responsibility for supporting regtech development, most importantly by creating IT and risk infrastructures that are capable of integrating these new solutions."

However, supervisors and regulators can support regtech's development by creating an enabling regulatory environment, a safe environment for FIs to share their challenges in compliance and regtech opportunities, and a platform for engagement between software developers, FIs and the public sector.

This report is based on the IIF response to the UK Financial Conduct Authority's "Call for input: supporting the development and adoption of regtech[2]," which we developed together with the members in our Regtech Working Group.[3] The IIF is the global association of the financial industry, with close to 500 members from 70 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks.

For more information on the IIF's regtech initiative, please contact Bart van Liebergen of the Regulatory Affairs Department (bvanliebergen@iif.com) or Conan French of the Innovations Team (cfrench@iif.com).

1 Institute of International Finance, "Regtech: exploring solutions for regulatory challenges," Washington DC, October 2015.
2 Financial Conduct Authority, "Call for input: supporting the development and adoption of regtech," November 23, 2015. See https://www.fca.org.uk/news/call-for-input-regtech.
3 For more information on the IIF's regtech and innovations work, see www.iif.com/topics/innovation.

EXECUTIVE SUMMARY

"Regtech" is "the use of new technologies to solve regulatory and compliance requirements more effectively and efficiently.[4]" While regtech solutions are already being applied by financial institutions (FIs), the current innovations in technology and areas such as "fintech" indicate that we are only at the early stages of a regtech market, with more development of new solutions in the near future.

The ambitious regulatory reform agenda implemented after the financial crisis has closed loopholes in the financial regulatory framework, but has also significantly increased compliance costs of FIs. In an uncertain macroeconomic and financial environment, applying regtech could make an important contribution to increasing the profitability and efficiency of FIs, while improving their effective compliance with financial regulations. By making compliance less complex and capacity-demanding, regtech solutions could free capital to put to more productive uses, increase competition by removing a barrier to entry, improve the quality and efficiency of supervision, and reduce risk in the system.

With the aim of stimulating the development of the regtech market, this report, based on inputs from IIF member firms, identifies main bottlenecks in compliance and regulatory reporting, discusses how they could benefit from regtech and from which regtech solutions in particular, and discusses barriers to regtech implementation and to development of the regtech market. The following issues in compliance and regulatory reporting could benefit from the development of regtech solutions:

1. **Risk data aggregation** as required for capital and liquidity reporting, for RRP and for stress testing, implies the gathering and aggregation of high quality structured data from across the financial group. It is complicated by definitional issues and the use of incompatible and outdated IT systems.
2. **Modeling, scenario analysis and forecasting** as required for stress testing and risk management is increasingly complex and demanding in terms of computing power and labor and intellectual capacity, due to the vast array of risks, scenarios, variables and methodological diversity that needs to be included.
3. A bottleneck in **monitoring payments transactions** (particularly in real-time) is the low quality and great incompatibility of transaction metadata churned out by payments systems. This complicates automated interpretation of transactions metadata to recognize money laundering and terrorism financing.
4. **Identification of clients and legal persons**, as required by know-your-customer regulations, could become more efficient through the use of automated identification solutions such as fingerprint and iris scanning, blockchain identity, etc.
5. **Monitoring a financial institution's internal culture and behavior**, and complying with customer protection processes, typically requires the analysis of qualitative information conveying the behavior of individuals, such as e-mails and spoken word. Automated interpretation of these sources would enable enormous leaps in efficiency, capacity, and speed of compliance.
6. **Trading in financial markets** requires participants to conduct a range of regulatory tasks such as margins calculation, choice of trading venue, choice of central counterparty, and assessing the impact of a transaction on their institution's exposures. Automating these tasks will ensure compliance and increase the speed and efficiency of trading.
7. **Identifying new regulations** applying to a financial institution, interpreting their implications and allocating the different compliance obligations to the responsible units across the organization is currently a labor-intensive and complex process, which could be enhanced through automated interpretation of regulations.

The report identifies several recent technological and scientific innovations and describes how they are, or could be, applied as regtech to help financial institutions comply with financial regulations.

1. **Machine learning, robotics, artificial intelligence** and other improvements in automated analysis and computer thinking create enormous possibilities when applied to compliance. Data mining algorithms based on machine learning can organize and analyze large sets of data, even

4 Institute of International Finance, "Regtech: exploring solutions for regulatory challenges," Washington DC, October 2015.

if this data is unstructured and of a low quality, such as sets of e-mails, pdfs and spoken word.[5] It can also improve the interpretation of low-quality data outputs from payments systems. Machine learning can create self-improving and more accurate methods for data analysis, modeling and forecasting as needed for stress testing. In the future, artificial intelligence could even be applied in software automatically interpreting new regulations.

2. Improvements in **cryptography** lead to a more secure, faster and more efficient and effective data sharing within financial institutions, most notably for more efficient risk data aggregation processes. Data sharing with other financial institutions, clients and supervisors could equally benefit.
3. **Biometrics** is already allowing for large efficiency and security improvements by automating client identification, which is required by know-your-customer (KYC) regulations.
4. **Blockchain and other distributed ledgers** could in the future allow for the development of more efficient trading platforms, payments systems, and information sharing mechanisms in and between financial institutions. When paired with biometrics, digital identity could enable timely, cost efficient and reliable KYC checks.
5. **Application programming interfaces (APIs)** and other systems allowing for interoperability make sure that different software programs can communicate with each other. APIs could, for example, allow for automated reporting of data to regulators.
6. **Shared utility functions and cloud applications** could allow financial institutions to pool some of their compliance functions on a single platform, allowing for efficiency gains.

Regtech could lead to great efficiency gains and more effective compliance at financial institutions; however, there are significant barriers to the implementation of most regtech solutions. We discuss the role of different stakeholders in overcoming these barriers. Financial institutions are key players in the further development of regtech; however, regulators can have an important role in promoting regtech implementation and development of the regtech market.

First, IT and data regulations, such as data protection or localization rules, can be an obstacle to effective information sharing across financial groups and lead to inefficient parallel "silos" of information in financial groups. IT requirements can increase the complexity of IT systems. For example, while Basel 239 requires centralization of IT systems, recovery and resolution plans require different parts of the system to be self-functioning in the event of resolution, thus requiring a decentralized system. Tight regulatory deadlines for IT updates amplify this problem by requiring financial institutions to tinker around the edges of existing infrastructures rather than allowing for a more fundamental overhaul of systems. Regulations can also complicate applying innovation other aspects of compliance, such as through requiring in-person identification instead of allowing digital identity verification methods.

Removing the existing legal and regulatory impediments to the sharing and use of data for regulatory purposes should be a priority for regulators. At the least, the FSB and international regulatory authorities should make a concerted effort to reduce such barriers, to remove inconsistencies of interpretation, and to achieve clarity among regulators and industry on how to manage the extent and impact of any such requirements that cannot be removed. The financial industry and regulators should also institute a dialogue on how regulations can unintentionally impact automation and innovation.

Second, a lack of data harmonization or insufficient detail of definition makes it hard to aggregate risk data across financial groups and jurisdictions on an automated basis. Many financial institutions still lack an integrated data dictionary and taxonomy, such as required by the Basel Committee's "Principles for effective risk data aggregation and risk reporting". However, global regulatory frameworks and financial infrastructures such as wholesale payments systems also differ widely in the definitions they apply to financial concepts and data. The financial industry and regulators across the globe should intensify efforts to standardize data and data sharing vehicles (such as through the LEI/UPI/UTI) and appropriately define regulatory concepts. We offer some examples.

Third, tight regulatory deadlines for IT updates require financial institutions to tinker around the edges of existing infrastructures rather than allowing for a more fundamental overhaul of systems. When regulators set more accomodative timelines for IT upgrades, that would allow institutions to focus on identifying and implementing innovative solutions

5 Spoken word can be analyzed by software applications when combined with natural language understanding technology.

and to adapt their infrastructures to new realities in a more fundamental way.

Fourth, some regulators still use outdated reporting portals and errors, creating inefficiencies and increasing chances of introducing error in reporting. Updating online reporting portals and secure data transfer mechanisms would significantly increase efficiency in the process both for regulators and FIs. Automated, secure online data transfer mechanisms without file size limitations could significantly increase reporting efficiency for both regulators and FIs.

Lastly, anti-money laundering and anti-terrorist financing (AML/ATF) surveillance would benefit from coordination and centralization, but is currently on a per-institution basis. That would require authorities to address current obstacles to the sharing of suspicious transaction reporting (STR) customer information, and other AML/ATF-related information.

As a last step, we discuss barriers to development of the regtech market. The regtech market is still in its infancy, with no dominant, widely used solutions yet emerged and financial institutions often still unfamiliar with new regtech solutions. Also, regulatory reform is not yet complete; uncertainty about the exact reporting requirements makes it harder for FIs to choose a particular compliance solution. As a result, FIs would benefit from a coordinated industry-wide design and collaboration effort to set clear standards for regtech in the product development phase, with all relevant regulators providing clear guidelines on the product requirements. Regulators should also provide as much clarity and speed as possible in communicating how compliance with particular regulations is required.

The regtech market is a niche market, requiring collaboration between unlikely partners: regulators and regulatory experts, technology and software developers, and entrepreneurs willing to invest. A coordinated effort or platform bringing together experts would enhance the entire community. To this end, the IIF has set up its Regtech Working Group. Regtech development is especially reliant on knowledge sharing between regulators, regtech ventures and financial institutions. Regulators could set up a regulatory supervisory hub to share knowledge on regulation, supervisory practice, and data formats, and create a "safe" environment for dialogue between the industry and its supervisors, for example through a "sandbox" approach.

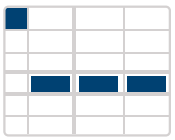
I. REGULATORY AND REPORTING REQUIREMENTS THAT WOULD BENEFIT FROM REGTECH

We have identified the following regulatory and compliance categories that would benefit in particular from regtech solutions. For each category, we explain which aspects are bottlenecks in compliance for financial institutions.

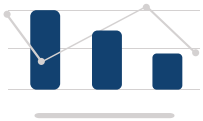
1. Risk data aggregation and management, and regulatory reporting[6]

Financial supervision is increasingly driven by data, with regulators requiring data of a greater granularity and at a greater frequency. The type of data needed to assess compliance with the majority of prudential regulations is called "risk data," which are typically quantitative and need to be of a high quality: structured, well defined, accurate and complete.[7]

The Basel Committee's "Principles for effective risk data aggregation and risk reporting," BCBS 239, set specific requirements for Global Systemically Important Banks' (G-SIB's) ability and internal infrastructure to aggregate risk data.[8] G-SIBs should be able to aggregate data largely on an automated basis and should have a dictionary of the concepts used in order to define data consistently across the group. In addition, they need to establish integrated data taxonomies and architecture across the group, "which includes information on the characteristics of the data (metadata), as well as the use of single identifiers and/or naming conventions for data including legal entities, counterparties, customers and accounts.[9]"



1. Risk data aggregation and management



2. Modeling, scenario analysis and forecasting

3. (Real-time) payments transactions monitoring, reporting and blocking (as for anti-money laundering(AML), anti-terrorist financing (ATF))

4. Identity verification as required by know-your-customer regulations

5. Monitoring employee and client behavior and organizational culture for conduct regulation

6. Real-time tasks for trading in financial instruments

7. Making FIs more aware of regulatory developments

6 For risk data aggregation, we adopt the Basel Committee on Banking Supervision (BCBS)'s definition: "defining, gathering and processing risk data according to the bank's risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite. This includes sorting, merging or breaking down sets of data." Source: Basel Committee on Banking Supervision, "Principles for effective risk data aggregation and risk reporting," Basel, January 2013, p. 9-10.
7 See for example Office of Financial Research, "Financial Stability Report 2015," Washington, DC, p. 69.
8 Basel Committee on Banking Supervision, "Principles for effective risk data aggregation and risk reporting," Basel, January 2013.
9 BCBS January 2013 B, principle 2.

IIF members have cited the following regulations as especially relevant to risk data aggregation:

a. Capital requirements such as Basel III and Solvency II require extensive reporting of portfolio risk data on which capital is calculated.

   i. Basel capital framework

      - The "advanced approaches" need data to validate and support the back-testing of models. Banks have made, and continue to make, huge investments in the necessary data and analytical IT. To take one example, regulation of interest rate risk in the banking book, which is now being added to Basel requirements, requires large volumes of aggregated data. Even the less-complex "standardized" approaches that in principle require less data but are likely to be used more widely under pending revisions of Basel III, will require accumulation, analysis and use of data to support inputs to the capital calculation. Banks are also required to capitalize for operational risk, and have been accumulating operational risk data to support modeling and analysis.

      - Basel 239 also has an important goal of improving banks' ability to provide aggregate risk information quickly and reliably to senior management and the risk function, to improve nimble decision making and risk control.

   ii. With Solvency II, reporting requirements for insurers have exponentially risen, with a solo quantitative reporting template (required quarterly and annually) now containing upwards of 75,000 data points. Meeting Solvency II data quality requirements is a challenge for insurers, with a recent survey indicating that one in five brokers view insurer data as "poor" and one in two as "average".[10]

b. Liquidity requirements under Basel III require banks to perform extensive calculations of their Liquidity Coverage Ratios[11] and Net Stable Funding Ratios[12] on an ongoing basis (with intraday liquidity reported daily[13]). Liquidity risk monitoring requires frequent, granular reporting for both direct and indirect clearing positions, name-based aggregation of counterparties, and, for the LCR and NSFR, application of mandated assumptions and haircuts to determine regulatory compliance.

c. Stress testing and risk assessments are based on extensive inputs of risk data as well as qualitative information.[14] Examples of risks assessed against defined adverse-risk scenarios are liquidity, credit exposures, risk weighted assets, balance sheet positions, and risk parameters. In addition, stress tests often assess qualitative aspects of an institution's risk management, such as capital planning procedures, operational risk, and expected material business plan changes.[15] Recent trends in stress testing include assessing the sustainability of business models.[16]

d. Recovery and Resolution Planning under the Financial Stability Board (FSB)'s Key Attributes of Effective Resolution[17], BRRD (UK, EU) and Dodd-Frank (US), require systemically important FIs to report in detail their main counterparty exposures and institutional structure. Depending on a firm's structure, the authorities may also require a firm to explain how its IT systems would support the reorganization of subsidiaries and business units, including possible divestitures.

e. Data gathering for OTC derivatives trade repositories[18] as mandated by the FSB's OTC derivatives markets reforms requires the reporting of information ranging from transaction economics, counterparty and underlier information, collateral, and operational data to event data.[19]

10 Insurance Times, "One in five brokers say insurer data is 'poor' – survey", 16 February 2016, http://www.insurancetimes.co.uk/one-in-five-brokers-say-insurer-data-is-poor-survey/1417370.article.
11 Basel Committee on Banking Supervision, "Basel III: The Liquidity Coverage Ratio and liquidity risk monitoring tools," (BCBS 238), Basel, January 2013.
12 Basel Committee on Banking Supervision, "Basel III: the net stable funding ratio," (BCBS 295), Basel, October 2014.
13 Basel Committee on Banking Supervision, "Monitoring tools for intraday liquidity management," (BCBS 248), Basel, April 2013.
14 Examples are the Bank of England's stress test, EIOPA stress tests, and the system stress tests executed by the International Monetary Fund (IMF) in its Financial Sector Assessment Program (FSAP).
15 Board of Governors of the Federal Reserve System, "Comprehensive capital analysis and review 2015 - Summary instructions and guidance," Washington DC, October 2014.
16 European Banking Authority, "Consultation paper: Draft guidelines on stress testing and supervisory stress testing," December 11, 2015, p. 29.
17 Financial Stability Board, "Key attributes of effective resolution regimes for financial institutions," Basel, 15 October 2014.
18 Trade repositories are entities that maintain a centralized electronic record or database of OTC derivatives data.
19 McIntyre, Alan, "Key themes to consider in ESMA's proposed revised EMIR RTS," Risk Focus, February 8, 2016, https://riskfocus.com/esma_l3_key_themes/.

Other regulations requiring reporting of detailed balance sheet items and positions are, among others, the FSB Data Hub (applying to the largest global banks), impairment detection under IFRS 9, large exposures measuring and controlling (BCBS 283[20]), operational risk requirements under Basel III, and credit and loan reporting such as for the European Central Bank (ECB)'s Analytical Credit Dataset (AnaCredit) and securities holding statistics (SHS).

Issues in aggregating, sharing and storing risk data

Many FIs currently face issues that impede the efficient, automated aggregation of risk data, and as such might benefit from regtech solutions. While regulations such as BCBS 239 require that risk data aggregation be mostly automated and centralized, in practice, IT challenges and regulatory and legal impediments often make the aggregation of risk data a manual, labor-intensive task.[21] IT problems in FIs often inhibit the efficient gathering of risk data from across the group. FIs usually have vast legacy IT systems, frequently consisting of older technology, built from multiple (sometimes incompatible) systems acquired through mergers and acquisitions in different jurisdictions. Regulatory and legal requirements may also lead to compartmentalization or "siloing" of systems, even though Basel 239 requires group-wide risk data aggregation. For example, recovery and resolution planning regulations may require systems to be able to function independently in different subsidiaries, to allow for an efficient resolution of the financial group.[22]

Data regulations can further complicate data aggregation. Data localization, security, protection and privacy rules may require that data from a subsidiary in a certain geography be stored and in some cases processed exclusively in that jurisdiction, leading FIs to manage data through decentralized warehouses. Compliance with requirements, such as customer authorization for use or transfer of data, also complicates development programs. There are specific restrictions on certain types of data, such as suspicious activity reports filed for Anti-Money Laundering purposes.

IT problems and data regulations can impede the efficient and timely sharing and gathering of data across the financial group and make it hard to update systems to comply with new regulatory requirements and data needs. This leads to less sensitive data being over-protected and under-analyzed because it is held in cumbersome datasets along with more sensitive data.

Lastly, the use of different definitions for central concepts in regulatory regimes in different jurisdictions makes gathered data hard to aggregate: if the definition of "short term debt" in one jurisdiction excludes repos but includes them in another, those figures cannot be aggregated in a meaningful way unless their definitions are harmonized. Internal or market-practice definitional differences can have the same effect, even where they do not reflect regulatory constraints.

Issues in filing data and information with regulators

Sending data and information to regulators is complicated when regulators use online portals requiring forms to be filled in manually, have file size limitations, or when they encourage the design of data collections as if they were reported using paper forms such as pdf documents. This is not only labor-intensive, but can introduce calculation error.[23] Slight differences in definitions, procedures, or technical requirements from agency to agency can add greatly to the difficulties of efficient definition and operation of data systems.

2. Modeling, scenario analysis and forecasting

Several regulations rely on the modeling and analytical capabilities of banks and insurers.

a. Capital and liquidity frameworks such as Basel III or Solvency II are based on internal or mandated models

20 Basel Committee on Banking Supervision, "Standards – Supervisory framework for measuring and controlling large exposures," Basel, April 2014. BCBS 283 requires banks to measure, aggregate and control exposures to single counterparties or to groups of connected counterparties across their books and operations. It should limit maximum losses faced in the event of a sudden counterparty failure to a level that does not endanger the bank's solvency.

21 See the BCBS' "Principles for effective risk data aggregation and risk reporting" or BCBS 239 of January 2013. In a recent monitoring exercise, no G-SIB fully complied with the Data Architecture and IT Infrastructure Principle of BCBS 239. Fewer than half of the participating G-SIBs rated themselves materially compliant. Source: Basel Committee on Banking Supervision, "Progress in adopting the principles for effective risk data aggregation and risk reporting," Basel, January 2015.

22 Financial Stability Board, "Recovery and resolution planning for Systemically Important Financial Institutions: Guidance on identification of critical functions and critical shared services".

23 OFR 2015, p. 72 and 74.

that estimate risks and capital needs. Liquidity requirements cover analysis and modeling of data against regulatory requirements on very short time horizons.

b. Stress testing and risk assessments require the modeling of the impacts of potential adverse external events (e.g. shocks in economic growth, inflation) on an institution's sustainability, solvency and liquidity. Examples are the Bank of England stress tests, the stress test and scenario analysis requirements in Pillar II of Basel III24, and macro stress tests executed for some IMF FSAPs. EIOPA conducts stress tests in the EU insurance sector.

c. Risk management and product development also rely on modeling to improve risk estimates and forecasts, and to improve the pricing or design of financial products.

d. Expected Credit Loss (ECL) accounting will introduce new modeling requirements, more extensive historical data collection, and new analysis of macroeconomic and other forward-looking data.25

e. Consumer protection requirements are developing rapidly in many countries, especially the UK and EU, and require analysis of customer suitability information, to avoid misselling or other problems.

In terms of modeling and analysis, stress testing is one of the most demanding supervisory requirements for FIs. FIs should use multiple perspectives and a range of techniques to achieve comprehensive coverage in their stress testing programs, including quantitative and qualitative techniques to support and complement the use of models.[26] Using a "suite of models and analysis" should reduce the test's vulnerability to excessive model risk.[27] A range of stress scenarios at the product, business and entity levels (including off-balance sheet vehicles) must be included, taking into account the performance of risk mitigating techniques. For illustration, a US investment firm needed each business unit to model the impact of 2600 macroeconomic variables on their revenue streams to identify the most critical variables to incorporate into the group's risk management models.[28] This warrants new approaches to data ingestion, model development and validation techniques.

First, to model the institution for current state, emerging, and hypothetical risk postures confidently, data must be constantly enhanced through automated ingestion and deployed or accurately mapped. Tagging the data components or metadata as it is streamed from the source systems into a central repository or repositories, aggregated as necessary, and filtered to the appropriate model or risk manager enriches the reporting and shortens the response time. Second, the modeling or analysis of such large data sources requires more powerful applications. Data sets covering several gigabytes of data with several million observations require distinct data mining tools and prediction tools, such as machine learning, for analysis.[29] Third, decentralized teams require the ability to communicate and collaborate effectively on highly complex quantitative risk management issues and articulate qualitative reports.

3. (Real-time) payments transactions monitoring, reporting and blocking; tax compliance

AML, ATF and sanctions regulations demand the monitoring and reporting of trades and transactions to regulators, and for banks to identify and flag suspicious transactions based on metadata in the transactions.[30] Banks both conduct post-facto checks on transactions (taking data inputs from loans, money market, payments and interbank systems), and monitor, flag and block or report illegal transactions in real-time.

The functioning of these systems is complicated by the fact that (international) payments are conducted on a multitude of different wholesale and intra-bank systems which are often incompatible with the information

24 Basel III's Pillar II approach includes the Internal Capital Adequacy Assessment, requiring banks to carry out a broad range of stress tests and scenario analyses relevant to their business models.

25 There are significant issues from the interaction of similar but divergent requirements, such as the need for adaptation of risk management parameters (probability of default, loss-given default) designed to calculate capital under the Basel III advanced approaches to the requirements of ECL provisioning under both IFRS and US GAAP accounting, such as stripping out regulatory conservatism and adding forward-looking information. The forward-looking information required for ECL accounting requires development of reliable, auditable techniques for reasonable and supportable use of scenario analysis and historical and economic data in the development of credit provisions. How ECL requirements will be applied to insurance companies remains to be determined in detail.

26 Basel Committee on Banking Supervision, "Principles for sound stress testing practices and supervision," Basel, May 2009.

27 Bank of England, "The Bank of England's approach to stress testing the UK banking system," London, October 2015.

28 Ayasdi, "Ayasdi Core – Accelerating the discovery of powerful insights from complex data," 2014. See also http://www.ayasdi.com/blog/bigdata/yesterday-ccar-less-stressful-citigroup/.

29 Varian, Hal, "Big data: new tricks for econometrics," April 14, 2014.

30 Examples are Anti-Money Laundering/Anti-Terrorist Finance standards designed by the Financial Action Taskforce (FATF) and administered under national law, and sanctions regimes enacted and enforced by, inter alia, the United Nations Security Council, the Office of Foreign Assets Control in the US, the European External Action Service (EEAS) in the EU, and the HM Treasury in the United Kingdom.

they provide on individual transactions. Lack of a single global payments standard means that different systems use different metadata or differ in their ability to attach metadata to transactions (such as through field size limitations). Transactions information in one system is noise to another system; for example, participants are generally unable to consistently and accurately identify country information in payment messages. These issues complicate the interpretation of transaction metadata for identifying suspicious transactions.

Similar issues arise under firms' efforts to comply with the US Foreign Account Tax Compliance Act (FATCA) and new global tax standards being developed by the Organization for Economic Cooperation and Development (OECD). These impose complex requirements to keep track of clients' identities, nationalities, and tax documentation, and to withhold tax in relevant cases.

4. Identity verification

AML/ATF/sanctions and tax compliance regulations also impose "Customer Due Diligence Requirements" (CDD). Know your customer requirements (KYC) are one of the key areas of financial regulation for CDD, requiring the identification of clients and business partners (both natural and legal persons, including beneficial owners) through analysis of different informational sources (both public and private) in different languages, and with sometimes differing definitions. KYC standards are often developed at a global level by FATF and administered and adapted under national law. KYC, however, is cross-border and is thus impacted at various levels by the intricacies and differences of jurisdictional interpretation and the interplay with ancillary regulation.

As such, there is a growing need, particularly in the business of correspondent banking, to create efficiencies of KYC without impeding the effectiveness of the process. KYC utilities, for example, have been developed or are being developed by several service providers with the aim of storing relevant due diligence information in a single repository. These platforms have considerable promise and banks are highly interested in the potential of such technological solutions; however, there also has to be a realistic assessment about confronting the hurdles to effective reliance upon such utilities.

Once again, cross-border restrictions on data transfer, storage, and usage are often hard to interpret but clearly make some vital information unavailable to certain entities under many circumstances, even to entities within the same group. Without resolving the problems created by such data restrictions, the KYC utility concept will remain unworkable in many situations.

A further fundamental issue is that banks will need some assurances that the regulatory, supervisory, and law enforcement authorities approve of the use of any such utility. Without such approval, much of the incentive to invest in and use them would be lost.

5. Monitoring behavior and organizational culture

Several regulations are relevant in this space:

1. Internal culture and conduct monitoring; rogue trading and other financial crime requirements, especially in the UK, EU and US.

2. Customer protection processes, such as meeting suitability requirements to avoid mis-selling and the processing of complaints, are labor-intensive tasks within FIs.

Compliance on these issues mostly concerns the analysis and management of qualitative information on decision-making and human behavior in the organization; tasks which are traditionally difficult to automate and are thus labor-intensive. Banks are still looking for ways to improve the efficiency and effectiveness of conduct and compliance surveillance. A trend is visible in conduct and organizational culture supervision towards the use of quantitative metrics as supervisory inputs. McKinsey has mentioned how some regulators no longer accept qualitative statements about how banks are introducing a stronger risk culture, but demand regular staff surveys that track progress and benchmark the bank against its peers.[31] In the UK, and to some extent in other countries, there is a good deal of emphasis on principles for "doing the right thing", which may further complicate the

31 McKinsey & Company, "The future of bank risk management," McKinsey Working Papers on Risk, December 2015.

data and IT aspects of compliance; on the other hand, the UK Senior Managers' and Certification Regime also imposes specific responsibilities on specific bank officers for designated activities, putting a premium on surveillance.

6. Real-time trading tasks

Multiple aspects of financial instruments and products trading are regulated:

a. Participants in financial markets need to manage their exposures and have appropriate risk management frameworks. In the US, for example, SEC rule 15C3-5 extends risk management requirements to all participants, including high frequency traders, by preventing market entry of orders exceeding pre-set credit or capital thresholds unless there has been compliance with all regulations on a pre-trade basis that the broker/dealer is restricted from trading. The EU's Markets in Financial Instruments Directive (MiFID) and MiFID II impose new and highly complex requirements to which both market intermediaries and underlying investors and counterparties must adapt. Full implementation of MiFID II, when it becomes effective, will create a suite of requirements, for which the means of compliance are still being built out by firms. In the US, banks also need to demonstrate that their trading desks operate in compliance with the Volcker rule; in the UK, the impending effectiveness of ringfencing under the "Vickers" regime will require somewhat similar monitoring.

b. Market infrastructures are regulated under MiFID II in the EU and UK, requiring trading to take place on multilateral trading facilities.

c. Financial instruments, and most prominently, derivatives, are generally separately regulated, such as in the EU's EMIR directive[32] and SEC/CFTC rules in the US for derivatives trading. These regulations encourage the standardization of OTC derivatives and require standardized derivatives to be cleared through central counterparties (CCPs). In addition, derivatives should report to trade repositories to improve the transparency of the market and protect against abuse. Uncleared derivatives require reporting to regulators and are subject to margin requirements and higher capital requirements.[33] Additionally, the EU's market abuse directive requires monitoring of transactions by financial instruments.

Effective and efficient trading on financial markets, subject to the regulations discussed, requires systems that are capable of processing these tasks in near real-time. In a trade these systems can calculate the impact on a trading desk's exposure of the trade to be executed; margin and capital requirements; and select a central counterparty through which to conduct the trade. Conformity with the firm's risk appetite and compliance with internal risk management requirements is also important.

7. Making financial institutions more aware of regulatory developments

Identifying new regulations applying to the organization, flagging their potential implications, and allocating the accompanying reporting and compliance obligations to the right organizational units is a complex task requiring significant capacity and human resources to interpret the regulations. Large FIs operating in multiple jurisdictions are faced with local, regional and global regulations that are constantly changing. It is challenging to keep track of the different regulations being promulgated, especially since regulators publish new regulations in different formats. Analyzing how regulations compare to each other, and on which points they are consistent, and then applying obligations in a coherent way within the institution is a particular challenge.

II. REGTECH SOLUTIONS

We have identified a number of technologies and techniques with value or potential in helping FIs report and comply.

1. Technologies improving data aggregation and management

Section I has illustrated how the efficient sharing, gathering and aggregation of risk data and qualitative

32 EU Regulation no. 648/2012.
33 BCBS, "Margin requirements for non-centrally cleared derivatives," Basel 2013; see also the G20 Pittsburgh and Cannes summit declarations.

information in FIs is typically met with challenges related to IT infrastructure and data regulations. The following new technologies could contribute to improving data management and aggregation:

New cryptographic and security technologies can benefit from information sharing by protecting privacy and ensuring data security and integrity, while improving the efficient disclosure of information to the relevant users, including regulators and users in subsidiaries across jurisdictions. Two classes of cryptographic tools may assist in balancing transparency and confidentiality: secure multiparty computation and techniques for achieving individual privacy in statistical data releases.[34] For example, Abbe, Khandani and Lo (2011) have developed a privacy-preserving method for sharing financial risk exposures based on secure multiparty computation.[35] It could be applied to the construction of privacy-preserving indexes of bank capital and leverage ratios, the monitoring of delegated portfolio investments, financial audits, etc.

Data Storage Cell Level Security is another application of cryptography to information sharing, which would enable only relevant and specific information be made available to individuals, based on his or her access authorization. The data's ingestion and parsing process would tag each unique metadata component by property, object, and access type, whereby eliminating the need to structure the raw data, instead enabling individuals with the ability to search across the entire data set.

Cell-level security capabilities help organizations overcome data security issues even for big data sets by applying access controls to every data object ingested into a common platform architecture. These labels are integrated with internal information security policies, user attributes, and enterprise authentication and authorization systems. The language or framework used to construct the security labels is expressive enough to handle complex visibility requirements without adding an excessive burden on existing authorization systems, and allows users to encode Boolean or natural readable language expressions and attributes. For example, analyst A in Country A is able to see Client C's name and account identifiable information and comprehensive activity, while analyst B in Country B is only able to see those aspects of Client C's information which has been disclosed by Country A outside its jurisdiction.

Cloud technology and open platforms enable the creation of **standardized shared utility functions**. Shared utilities could provide a service for different subsidiaries within a single FI, such as a central data repository on the cloud. When shared utilities provide services to multiple organizations across the industry (such as a KYC utility), it would enable banks to optimize their core processes and benefit from greater economies of scale for services that do not need to be in-house. They could reduce cost, increasing scalability and flexibility for regulatory and compliance applications. Industry utilities could also drive standardization of data and simplification for regulatory compliance. Of course, utilities will present their own challenges, including confidentiality, security, maintenance, reliability, and data quality (including standards for how up-to-date data must be).

Data mining algorithms based on machine learning could help with organizing (and analyzing) large volumes of unstructured data through their ability to identify complex, nonlinear patterns in large data sets. Unstructured data refers to data without the well-defined and consistently applied schemas or constraints on data types, storage formats, and allowable values that facilitate automated analysis. Data mining algorithms are typically highly efficient for exploring high-volume or high-dimensional data. The algorithms are typically also designed for generic application and can process unstructured data.[36]

Lastly, **blockchain** is transparent by design and could be a mechanism to give regulators direct, instant and full transparency of information in FIs. Since all transactions are documented on the distributed ledger, a comprehensive, secure, precise, irreversible, and permanent financial audit trail could exist for regulators. Reporting could be replaced by regulators' participating in an appropriately permissioned transaction-related distributed ledger. This near real-time view of all transactions would enable regulators to better analyze systemic risk. Many argue that blockchain could potentially replace the centralized clearance and trade reporting of contracts as a mechanism to provide transparency of transactions. But many questions, including the adaptability

34 Flood, Mark, Jonathan Katz, Stephen Ong and Adam Smith, "Cryptography and the economics of supervisory information: balancing transparency and confidentiality," Office of Financial Research Working Paper no. 0011, September 4, 2013.

35 Abbe, Emmanuel, Amir Khandani and Andrew Lo, "Privacy-preserving methods for sharing financial risk exposures," November 19, 2011. Paper available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1962090.

36 Flood et al. 2014, p. 9.

of blockchain to high-volume, real-time uses, but also the degree of standardization of systems and data required, remain to be examined.

What is more, a system where the supervisor has direct access to all individual transactions raises a myriad of questions about confidentiality for customers, data security, and as a result, such a system's morality; about governance of the supervisory process; supervisors' capabilities to receive and process data; and, most of all, about the proper roles of supervisors, on the one hand, and firms' managements and risk functions, on the other, in overseeing market functioning and compliance. Data sharing should not enable third parties to identify particular clients. It may be useful to start such a discussion, provided that ample time is provided for full ventilation of all the many issues that would come up.

2. Technology for advanced data analysis and interpretation

In section I, the report has identified several areas in which advanced data analytics could be applied. New technologies could in particular help with improving and back testing risk models, creating more accurate and granular statistical analytical methods, interpreting unstructured and qualitative data outputs, such as from payments systems, from surveillance of communications and behavior, or transaction patterns that may be suspicious; and in "understanding" new regulations. We briefly discuss technologies and techniques in more detail below.

Machine learning identifies complex, nonlinear patterns in large data sets and makes more accurate risk models. By adjusting algorithms based on newly acquired information, their predictive power improves through use. This has several potential applications in compliance. In stress testing and risk management, it would benefit definition of models, the calculation and simulation of stress scenarios, and improve the accuracy and granularity of statistical analyses. New types of models developed through machine learning offer deeper insights into data than previously possible. For example, Khandani, Kim and Lo develop a method to improve consumer credit risk models through machine-learning algorithms.[37] It could also be applied to automate name-based aggregation for large exposure regulations.

Robotics can further automate the control of other IT processes including machine learning, data flow and storage to enhance speed and efficiency, and minimize human error.

A major application of machine learning is in **analyzing unstructured data**, which has briefly been introduced above. Analysis and interpretation of unstructured data inputs, such as e-mails, spoken word, pdfs and metadata, could benefit several areas of compliance.

- Handling customer protection and complaints could be improved by automating suitability analysis and procedures designed to avoid mis-selling, and several of the steps from customer complaint to internal action or response: the collection of complaints, escalation of those complaints requiring substantive action, analytical capabilities to perform root-cause analysis.
- Monitoring behavior and internal culture in organizations can benefit from coupling unstructured data analysis with **natural language understanding technology**, which could forego the need to have personnel listen in on internal phone conversations. When combined with new machine learning tools, automated systems can be allowed to interpret unstructured data inputs such as automatically generated phone call transcripts, e-mails and pdfs to recognize patterns instead of key words and integrate with other data points. Key word filters are demonstrably inefficient since they produce "false positive" problems as also encountered in, for example, sanctions screening for names.
- Know-your-customer regulations require identification of customers, which could be automated through machine learning and advanced analytics; similarly, transaction monitoring for suspicious transactions or sanctions could benefit.
- "Regulatory radar" software could capture the flow of new regulations in a single database with all obligations, allowing a firm to assess the applicability of regulations for the firm, and flagging issues of interpretation for closer examination. It could then compare the regulations as required to the firm's current compliance

37 Khandani, Amir, Adlar Kim, and Andrew Lo, "Consumer credit risk models via machine-learning algorithms," Journal of Banking and Finance, 2010, 34(11).

processes and to existing regulations for any overlap to identify if any potential changes are needed. In turn, it should ensure that obligations arising from new regulations are allocated to the relevant organizational unit. Such software could run on **cognitive computing** in order to understand texts.[38] As an alternative to using cognitive computing to attempt to interpret unstructured regulatory publications, **machine readable regulations** can help standardize the publication and consumption of regulations, reducing ambiguity and interpretation errors through the use of standardized rulesets.

Visual analytics is the science of analytical reasoning enhanced by interactive visualizations tightly coupled with data analytics software. This could combine visualization's "high-bandwidth information channel to the human analyst with the flexibility and power of rapid-iteration analytics[39]," improving the interpretation of data. This could especially have merit in complex analyses as needed for stress testing.

When coupled with **biometrics technology** to enable fingerprint and iris scanning, face recognition, but also remote passport recognition and eIDs, advanced analytics can allow for more efficient ways to verify an individual's identity to access financial services.

3. Technologies allowing for real-time compliance and risk management

Powerful calculation engines allowing for real-time risk management, collateral management, and views of portfolio exposures and risks have been around for a while.[40] FIs are also increasingly relying on real-time computing power to conduct derivative trades quickly and efficiently in compliance with regulations, with the engines calculating such aspects of transactions as the required margins and the selection of central counterparties.

Real-time analytical capabilities are increasingly enabled by **cloud analytics**, an integrated technology architecture that streams and fuses different data types at gigabyte to petabyte scale, powered by cloud computing power with advanced predictive analytical capabilities. Combining these technologies into a regulatory framework transcends the limits of other forms of analysis and delivers insights to answer previously unanswerable questions resulting in real-time analysis capabilities.[41]

4. Other technologies

Two technologies have potential uses in compliance and reporting across the board. We briefly discuss blockchain/distributed ledgers and Application Programming Interfaces (APIs) below.

Blockchain / distributed ledger technology

Distributed ledger technologies such as blockchain stand out for the wide range of applications they could offer and as such, merit a separate discussion. The blockchain is a distributed consensus system that enables transactions to be quickly validated and securely maintained through cryptography, computational power, and network users, removing the need for a trusted centralized authority. The distributed public ledger, or database, contains time-stamped and irreversible information of all transactions that is replicated on computers around the world, thereby eliminating a single point of failure. While the blockchain is most often referred to in the context

38 Cognitive computing uses a superset of such applications as machine learning, neural networks, natural language processing and behavioral intelligence, to solve complex situations characterized by ambiguity and uncertainty. IBM has defined it as "systems that learn at scale, reason with purpose and interact with humans naturally."

39 Flood, Mark, Victoria Lemieux, Margaret Varga and William Wong, "The application of visual analytics to financial stability monitoring," Office of Financial Research Working Paper 14-02c, May 9, 2014.

40 Opelia, Nancy, "Real-time risk management: prime brokers are racing to upgrade infrastructure and core technology," CFA Magazine January-February 2006.

41 An integrated real-time analytics technology architecture incorporates the necessary technology platform, either a public or private cloud, a single secure data repository, a high-throughput low latency ingestion pipeline, powered by analytical tools that can be manipulated by compliance professionals with the relevant data science skills to create customizable data visualizations.

of the Bitcoin platform, it is not technically dependent upon it. Other applications can, and have, incorporated the technology. Moreover, innovation is ongoing and a wide range of alternative distributed ledger models are being developed.

Because virtually any type of information can be digitized, codified and placed onto the blockchain, a database that is, in principle, tamper-proof, permanent, and whose validity is confirmed by the consensus of a community of computer users—rather than by a central authority—, the technology has potential to impact the finance industry:

- Software-automated transactions or "smart contracts" have the potential to increase transparency of financial contracts, reduction of settlement and systemic risk, increase post-trade efficiency and unlock capital through real-time settlement. Smart contracts, data chronology and cryptographic immutability are well suited to compliance and audit requirements, and therefore should be acceptable to supervisors, provided good controls and governance are in place.[42]
- Digital identity on the blockchain could enable timely, cost efficient and reliable KYC checks or verification that individuals or organizations have appropriate regulatory approvals and licenses.
- Near real-time settlement could be achieved through automation and global consensus on the blockchain. These capabilities could automate compliance aspects in use cases including cross-border payments, syndicated loans, and repo markets.

Of course, it should be acknowledged that the practical application of blockchain in regtech solutions still has hurdles to overcome, such as its currently limited scalability and speed of execution.[43]

Application Programming Interfaces (APIs)

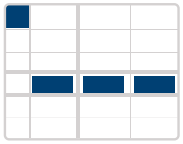
An application programming interface (API) is a particular set of rules and specifications that software programs can follow to communicate with each other and facilitates their interaction. The open character of APIs (being published publically) encourages integration standards and innovative use of their functionality. Banks can develop and share APIs for regtech firms to build from and regulators can create APIs for compliance submissions along with service level agreements (SLAs) which are common in industry. This standardization and automation could begin with some of the following actions:

- Regtech to construct, manage and communicate APIs. At this stage, regulators should preferably leave banks maximum flexibility in applying APIs. We may need to develop a common standard for API contracts, their management and registration and their usage over time, but for the moment regulatory guidance as to requirements should aim to "let 1000 flowers bloom" and ideally allow the market to develop compliant approaches to managing APIs that work for FIs and users alike.
- There is a need to construct, manage and communicate the data content for APIs. This could be extended to existing industry interfaces, including those for reporting to regulatory authorities. The existing message standards (e.g. SWIFT) still require a great deal of manual message construction. And regulators are still completely proprietary in their interface contents (e.g. for transaction reporting). Regtech could ultimately develop and implement globally consistent definitions, support interface construction, and provide a comprehensive testing suite. Official endorsement of consistent definitions will probably be in order, although at the right stage of the progress, once the direction of innovation and clear needs for such endorsement are established.
- Security for public APIs or business-to-business (B2B) and business to-consumer (B2C) interfaces is also often questioned. A common regulatory framework platform could increase security for these APIs.
- Standard reporting utilities that incorporate standard interfaces and protocols, automated, near real-time, message-based, continuous (not "a point in time" reports), trusted source of data, system generated could make regulatory reporting more efficient and timely.

42 For more information, see for example Flood, Mark, and Oliver Goodenough, "Contract as automaton: the computational representation of financial agreements," Office of Financial Research Working Paper 15-04, March 26, 2015.
43 Fest, Glen, "Can blockchain tech really unclog the capital markets?" American Banker, February 24, 2016.

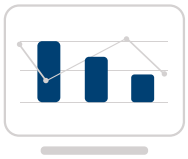
ISSUE	REGTECH SOLUTION

Risk Data aggregation and management



- Cryptography, cell-level security, data ingestion and information sharing technology, and potentially blockchain for improving data management, security and aggregation in and between institutions and with regulators
- Machine learning and advanced analytics (including potential use of quantum computing) for organizing large volumes of structured and unstructured data
- Open platforms and networks to help build a robust standard data dictionary across the industry
- Better automated and secure online data reporting portals from regulators, running on compliance APIs

Modeling, scenario analysis and forecasting



- Machine learning, advanced analytics and new types of models can improve modeling and data analysis
- Data storing, access, sharing and aggregation techniques as above
- Modern data visualization techniques for improving interpretation of data, and advanced data analytics

(Real-time) payments monitoring, reporting, blocking

- The blockchain could have potential as a substitute to existing, tiered payments systems
- Machine learning to interpret unstructured (meta)data outputs of payments systems, such as the identification of payments beneficiaries

ISSUE	REGTECH SOLUTION

Identity verification

- The blockchain is already used as a mechanism for digital identity verification and may develop in the future into a secure information sharing system
- Data mining, natural language processing, and visual analytics for the processing and analyzing of unstructured data may be able to provide an operational solution to solve for client onboarding.
- Encouragement of biometric, social verification, or other new means of identity verification, especially in emerging markets

Monitoring behavior and organizational culture

- Unstructured data analytics combined with voice-to-text capabilities to improve communications surveillance, recognize behavioral patterns from data and, for example, to make rapid consumer suitability determinations

Real-time trading tasks (financial markets trading)

- Machine learning and predictive analytics for markets trade surveillance
- Real-time margins calculating, CCP choice and risk management engines, compliance monitoring, end-of-day reconciliation of all transactions, and reporting for derivatives trading
- The blockchain may develop into a substitute for current trading platforms

Making financials more aware of regulatory developments

- Cognitive computing / deep learning techniques that enable "regulatory radar" software with understanding of regulations

- Additionally, a Secure Mechanism for File Transfer could be adopted by the major international financial regulatory bodies with the Joint Worldwide Intelligence Communications System Intranet (JWICS) as a model. The JWICS is the intranet run by the U.S. Department of Defense and used across the intelligence community to transmit classified and sensitive information. Encrypted file transfer protocol infrastructure is currently utilized by various US regulators.

III. IMPLEMENTING REGTECH IN FINANCIAL INSTITUTIONS: BARRIERS AND SOLUTIONS

1. Obstacles in regulation and legislation

Restrictions on the use of data and new technologies can be outdated, while creating inefficiencies and complexity in risk and IT infrastructures. Regulations and laws impact FI's use of data and (new) technologies in many ways. They can curb the use or sharing of certain data, require certain activities in an FI to be automated, or designate activities that should not be done in automated ways, and create other requirements for data and IT infrastructures. Fis deal with a variety of regulations internationally in regard to data and IT; among others

- Data privacy and data protection rules, protecting the privacy of individuals in data use
- Data security requirements
- Data localization requirements, which require data to be stored on local servers
- Basel 239's principles on risk IT infrastructures, requiring centralized and automated aggregation of risk data in banking groups (G-SIBs and D-SIBs)
- Recovery and resolution requirements on critical IT and risk infrastructures
- Know-your-customer regulations, requiring specific methods for identification

As technologies change, it is important that regulations remain up to date in the sense that they still attain their ultimate goal, while not unintentionally obstructing new possibilities in technology.

Data protection, privacy and localization requirements

With regard to data rules, protecting the confidentiality of clients' data and ensuring security when transferring these data is crucial for FIs. Legislation and regulation on data is important to protect the privacy of individ¬uals and assure the appropriate use of sensitive or personal information. At the same time, restrictions on the ability to use data across national borders may impact the ability of FIs to rely on big data or advanced analytics solutions. Policymakers should continuously reassess the impacts of technological developments on data security and privacy, ensuring that regulations strike an appropriate balance between protecting privacy and security, and effective data use.

Removing the existing legal and regulatory impediments to the sharing and use of data for regulatory purposes should be a priority. At the least, the FSB and international regulatory authorities should make a concerted effort to reduce such barriers, to remove inconsistencies of interpretation, and to achieve clarity among regulators and industry on how to manage the extent and impact of any such requirements that cannot be removed.

IT infrastructure requirements

The requirements imposed on FI's IT infrastructures are not necessarily consistent or compatible across regulations. Definitions, granularity requirements, formats, and the like vary from regulation to regulation, even within the same jurisdiction. Ad-hoc information requests often pose additional challenges. Regulatory goals may also differ. For example, on the one hand, Basel 239 requires group-wide risk data aggregation. On the other hand, recovery and resolution requirements for systemically important FIs identify IT systems such as data storage and processing, telecoms, servers and data centers, and risk management functions such as central risk management as "shared services" that could be critical to the functioning of an institution. When designated as critical shared

service, they should be resolvable and able to function independently in case of resolution.[44]

This may contribute to difficulties in overcoming the "siloing" of legacy IT and risk reporting infrastructures. Silos, separated reporting and IT structures within Fis, impede the sharing and gathering of data across the organization and can lead to double work, with data on the same phenomenon potentially collected in slightly different form.[45]

Promoting automation in compliance and reporting procedures

Regulations could acknowledge the role of new technology in the kind of compliance they require, subject of course to the condition that the reliability and security of these technologies has been proven. Most clearly, digital identity verification requires regulatory coordination on the cross-border use of eIDs and eSignatures for digital on-boarding and transactions. Current regulations on the prevention of money laundering and terrorism financing should be assessed to allow ex-post validation of alternative online identity verification mechanisms (biometrics, video call, third-party verification). Regulation needs to be digital-friendly, i.e. without requiring physical signatures and other physical elements in the KYC process.

In the long term, new regulations could be formulated in machine-readable code so that new rules can be applied automatically in FIs, improving the speed, efficiency and effectiveness of new rule implementation in the financial sector.

Financial services organizations would also benefit from the availability of an industry wide regulatory taxonomy that applies across countries and legislations. It should cover same or similar regulations coming from different regulators and will help ensure compliance by matching the implementation with relevant laws, regulations or rules (including private financial market infrastructure rules or listing requirements), etc.

Most importantly, when developing compliance and reporting requirements and processes, it is essential for regulators to consult the industry to make sure that efficiencies are maximized and problems are avoided to the extent possible. They should also make it a rule in all cases to consult their international peers, so that as much international consistency and compatibility as possible is built in from the beginning, rather than creating burdensome differences that will be hard to correct in the future.

2. Data harmonization and definition issues

A lack of data standardization and harmonized definitions of key reporting concepts impedes the aggregation of risk data in FIs from across subsidiaries and geographies. Definitions of data and key regulatory concepts differ widely internationally, be it in payments systems or in regulatory frameworks, even though certain regulatory regimes are negotiated at the international level. This complicates the aggregation of data originating in multiple jurisdictions at an enterprise level, whether by automation or manually. Importantly, the heterogeneity of national requirements and regulations makes it unattractive to develop solutions that cover national regulatory requirements unless the developer reaches a critical mass.

There currently are a range of public and private data standardization and definition harmonization initiatives running, such as the LEI/UPI/UTI and ISO20022. Nevertheless, diversity of data standards and definitions remains an issue and the stability and efficiency of the global financial system would greatly benefit from further harmonization initiatives at an international level. Of course, technology and data requirements change swiftly; as a result, regulators could best push for standardization of those data requirements that have been well-established in practice while still keeping a more open approach to new data concepts.

Harmonizing data standards

Data standards are documented agreements on how to define, represent, format, or exchange data. Standards enhance data sharing, enable integration, and help address coordination challenges posed by regulatory fragmentation. Standards also help firms create higher quality data for internal risk management and regulatory reporting, shortening the lag between market developments and regulators' understanding of them. To maximize

44 Financial Stability Board, "Recovery and resolution planning for Systemically Important Financial Institutions: Guidance on identification of critical functions and critical shared services".

45 European Central Bank, "Central banking statistics – New opportunities for innovation and cooperation," Presentation at World Statistics Day event, Budapest, October 21 2015.

their benefits, data standards should be developed and applied globally through partnerships between the public and private sectors.[46]

Regulators and industry across the globe could work together to introduce data standards where they are currently lacking, and improve existing data definitions where necessary. Several types of standards could be thought of (a number of standardization initiatives are already running; they are mentioned below):[47]

- The Legal Entity Identifier (LEI) identifies specific legal entities and is required to manage relationships, which could include parent companies and their subsidiaries as well as off-balance-sheet vehicles.[48]
- Product identifiers identify groups of financial instruments according to shared properties or intrinsic characteristics. Importantly, the Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO), with substantial input from the International Swaps and Derivatives Association (ISDA) supported by the IIF, is currently working on a Unique Product Identifier (UPI).
- Instrument identifiers identify specific financial instruments such as stocks, bonds, and loans. An example is the International Securities Identification Number (ISIN), which was developed in the 1980s and may need updating.
- Transaction standards identify information used in financial transactions. The CPMI/IOSCO proposal for a uniform global Unique Transactions Identifier (UTI) is a good example of a transaction standard for OTC derivatives. Wholesale payments systems, which differ widely in the type and possibilities for metadata included in financial transactions, are also in need of standardized transactions information to allow for better automated cataloging and understanding of transactions.
- Another transaction standard is ISO 20022, or the "universal financial industry message scheme," an open methodology for developing new financial messaging standards and for harmonizing existing messaging standards. ISO20022 has been adopted by several exchanges and payments systems, and more will follow.[49] It is important primarily for providing universally-agreed upon definitions that can be applied for business, legal, and technicians. How broadly it should be applied remains, however, subject to debate.
- Standards for financial and business reporting identify information reported by companies in financial disclosures and regulatory reports. An example is XBRL, which enables free and open exchange of business and financial information.

Consistent data standards should allow regulators to build data repositories and reporting requirements with data requirements and definitions which are consistent with those of others. Even more importantly, national regulators should consult and agree – after appropriate consultation with the industry on an international basis – on harmonized requirements before launching into new requirements or new repositories.

In the case of the FSB Data Hub, the FSB and the Hub have been good about consulting the industry for input; however, the effort of consultation and refinement will need to be continued as the Data Hub gains experience and as its requirements expand. Every effort should be made to make reporting requirements as consistent as possible with international data and reporting standards.

Harmonizing data definitions

Differences in regulatory definitions should be identified in a comprehensive manner and harmonized as a much as possible in order to enable the use of regtech solutions. While some differences in definition will naturally persist to some extent ("retail" may have a different meaning for liquidity or capital adequacy purposes) such differences should be avoided or at least minimized.

46 OFR 2015, p. 69. Several initiatives of the Enterprise Data Management (EDM) Council, an association founded by the financial industry to elevate the practice of data management as a business and operational priority, promote data standardization. EDM has initiated among others a Financial Industry Business Ontology (FIBO), Data Management Capability Assessment Model (DCAM), and data quality initiatives. http://www.edmcouncil.org/.

47 Categorization from the Office of Financial Research, "2015 Financial Stability Report," p. 69.

48 See the website of the Global LEI Foundation, www.gleif.org.

49 In the US, the Fed has declared an intention to implement ISO 20022 for US payments and DTCC is using it for its Corporate Actions service. It is also used by the Chinese domestic payments system, CNAPS, the Japanese securities depository JASDEC, the Singapore stock exchange (SGX), the Australian stock exchange (ASX), and it has been chosen as the standard for the forthcoming Australian real-time payments system. ISO 20022 is also the standard used for messaging by strategic initiatives such as the Single Euro Payments Area (SEPA).

The granularity of reporting should also be addressed. It needs to be recognized that if requirements are not adequately defined at initial finalization of a regulation, changes will be costly and time consuming. For example, any additional layer that has not been included in a final reporting format takes a minimum 12 months to implement in an automatized format.

Harmonizing definitions of key regulatory concepts would benefit regtech development but would also allow banks to better integrate their internal data processes into single data warehouses or repositories. To effectively use internal data for reporting and management purposes, FIs need access to a central data repository or interface to be able to aggregate risk data from across the financial group. Risk and reporting requires the ability to search for data from multiple databases and then turn that wholesale data into statistical, relational, geospatial, and behavioral analysis. Compiling the relevant data from the source systems must be at category level (product, country, client business sector, etc.) where analysts will review the collective data to identify hidden or previously unknown relationships and patterns.

The following examples show how differences in definitions between regulatory frameworks or jurisdictions complicate regulatory compliance:

- "Short term interbank funding" is based on a 3-month horizon for risk-weighted assets computation in Basel III, while it is based on "less than one year" threshold in the net stable funding ratio.
- "Asset encumbrance" definitions are equally unaligned across regulations.
- "Wholesale funding" definitions differ across requirements. For example, liquidity ratios define wholesale funding as opposed to retail funding.
- "Retail counterparty" definitions differ across regulations, though sometimes for good reasons. A small business customer would be considered a retail customer for the purpose of Basel liquidity regulation if the funding raised from that client does not exceed 1 million euros. However under Basel capital regulations, the funding amounts are not a criterion for assigning small business customers.

Regulators should be clear on which reporting should be formally reconciled with accounting numbers. Accounting reconciliation is often complex and should only be required where there is a real need for it. For example, the LCR is a monthly early warning indicator. As such its full accounting reconciliation would result in undue operational complexity.

Regulators around the world have been working to harmonize data. In 2013, the UK's FCA and PRA concluded a memorandum of understanding on data, aiming to avoid duplication of regulatory data requests to FIs.[50] Also, several ECB initiatives, currently run by the ECB's Directorate General Statistics, provide an example of harmonizing data definitions in multiple ways. Banks' Integrated Reporting Dictionary (BIRD) will be a set of documentation aiming to provide a standardized model for organizing the internal data warehouses of banks in an integrated way without adding reporting requirements. The Single Data Dictionary (SDD) should integrate the methodology and semantics of existing European frameworks. Lastly, the European Reporting Framework (ERF) should become an integrated and harmonized cross-country reporting scheme for banks, covering most existing reporting requirements of both the ECB and the European Banking Authority (EBA).[51]

This kind of initiative could help supervisors receive data of a better quality at the source, leading to a more efficient and less costly report production and a "univocal interpretation and clarity of regulations.[52]" Such initiatives need to be paralleled on the international scale insofar as possible, perhaps through the Basel Committee. The ECB should make it a priority to ensure that its initiatives are made as consistent as possible with global standards and definitions.

3. Regulatory deadlines for IT upgrades

Implementation deadlines of regulations can be unrealistic – particularly when they have far-ranging impacts, such as the local implementation of FSB derivatives reforms, MIFID II, and EU Data Protection Regulation. Short

50 www.fca.org.uk/firms/systems-reporting/common-data
51 Schubert, Aurel, "Data as a core central banking asset – the strategy of the ECB," Presentation given at the Swedish Riksbank's Big data workshop, 9-9-2015.
52 Idem.

MAIN BARRIERS TO THE IMPLEMENTATION OF REGTECH AND FOR DEVELOPMENT OF THE REGTECH MARKET

Impediments for the regtech implementation

Legal restrictions on the use of data and new technologies

A lack of data standardization

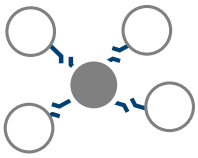
Regulatory deadlines for implementing new IT solutions in FIs

Outdated reporting portals and methods used by some regulators

Impediments for the regtech market (next section)

Uncertainty due to still unfinished regulatory agenda

The preliminary stage of the regtech market



Lack of networks bringing together regulatory experts, software developers and FIs.

deadlines can force FIs to comply through tinkering around the edges of existing (legacy) infrastructures with suboptimal outcomes, rather than through fundamental overhauls of their IT systems. Some appropriate realism has been shown in applying requirements under Basel 239, but the problem of short and overlapping deadlines remains a real one. Requirements such as Basel 239 create important incentives for banks to modernize systems to current regulatory needs, but the multiplicity of requirements can create headwinds, especially when combined with needs to adjust systems to changing business models and new technological challenges.

More time to meet regulatory technical requirements would allow institutions to focus on identifying and implementing innovative solutions and to adapt their infrastructures to new realities in a more fundamental way. When supervisors set better deadlines, or make these deadlines part of a larger effort to allow FIs to overhaul their IT systems, outcomes both for FIs and supervisors could be optimized.

4. Outdated reporting portals and methods used by some regulators create inefficiency and increase chances of introducing error.

Responding to the regulators with qualitative reports and large data sets can be labor-intensive, inefficient and prone to error when regulators use online portals requiring forms to be filled in manually, or when they encourage the design of data collections "as if they were reported using paper forms[53]" such as pdf documents.

Updating online reporting portals and secure data transfer mechanisms would significantly increase efficiency in the process both for regulators and FIs.

Automated, secure online data transfer mechanisms without file size limitations could significantly increase

53 OFR 2015, p. 72 and 74.

reporting efficiency for both regulators and FIs.[54] Standardization of these processes across different regulators and jurisdictions would further enhance efficiency and speed. Sharing data is easier when regulators work together in designing financial data collections to apply standards and develop automated sharing mechanisms.[55]

Automating data transfers also minimizes the potential for human or manual error. Although many regulatory agencies have been working toward using XBRL, or eXtensible Business Reporting Language, agencies continue to define data requirements pursuant to their own legal systems, IT systems and preferences, whereas greater international consistency and compatibility would greatly improve both the cost-efficiency and the reliability of reporting.

Financial services organizations would benefit from availability of standardized communication mechanisms (data formats and definitions, APIs, protocols) across different legislative and regulatory requirements. A single, streamlined communication protocol would increase the consistency of the reports, enhance the comparability across different standards, regulations and legislation, and reduce the efforts and costs associated with regulatory compliance.

5. Analytics for identifying suspicious transactions

There is a need for more industry collaboration on analytics to identify and report suspicious transactions for AML/CTF and sanctions compliance, and for an improvement in pattern recognition across institutions. Currently, surveillance is on a per-institution basis; coordinated or centralized surveillance could significantly improve efficiency and effectiveness in recognizing suspicious trades. However, progress in this area will require the authorities to address current obstacles to the sharing of suspicious transaction reporting (STR) customer information, and other information that would be useful to more effective AML, CTF and sanctions compliance.

IV. THE REGTECH MARKET: BARRIERS AND SUGGESTIONS FOR DEVELOPMENT

With products based on new and recent technology, the regtech market is still a "young" market, with many ventures existing for only a couple of years or less. While regtech is roughly based on the same technological innovations as fintech, the fintech market has seen more explosive growth. Indeed, several factors, rules and policies could act as barriers to the development, adoption and implementation of regtech for financial services. Below, they are briefly discussed, as are potential policy measures to overcome these barriers.

1. A still-changing regulatory landscape creates uncertainty on upcoming reporting requirements, making it hard for FIs to choose a particular compliance solution.

FIs have a disincentive to invest in a particular software solution when the regulations for which it provides compliance could still change. Acquiring and implementing regtech or any software solutions in the existing infrastructure is typically costly, so institutions need to be sure an investment is for the longer term.

2. The preliminary stage of the regtech market means that no dominant, widely used solutions have yet emerged. Also, FIs are often still unfamiliar with new regtech solutions due to their short history.

When technological solutions become more widely adopted, their use provides clients and sellers with economies of scale: for example, use of the same technology by clients' counterparties could bring benefits in data sharing, maintenance of the technology, etc. For these reasons, the preliminary stage of the regtech market could keep FIs from investing in a particular regtech solution. The short existence of most regtech also implies that many FIs are still unfamiliar with its possibilities, reliability, and acceptance, creating another barrier in regtech procurement.

54 In the case of the FCA, file transfer is particularly problematic when attempting to send large files outside of the FCA's GABRIEL systems due to file size limitations at both firms and the regulators. An updated, secure file transfer mechanism would have the added benefit of the FCA being able to put document request lists onto this system with firms loading the right document against each document requested. For example, the FCA requests the 'latest firm risk assessment document for AML' and it would allow FIs to load the latest AML ORAP against this. This reduces administrative burden at both ends through the clarification of document provision.

55 OFR 2015, p. 73.

Many FIs have relied on in-house built applications; changing to market-supplied software could require a cultural shift within the organization.

FIs would benefit from a coordinated industry wide design and collaboration effort to set clear standards in the product development phase, with all relevant regulators providing clear guidelines on the product requirements. This would allow regtech firms to compete to provide compliant products that banks could select to meet the needs of their business models. The current product development life cycle is based on adoption of emerging solutions but the required critical mass takes time.

3. Lack of networks or platforms bringing together regulatory experts, software developers and FIs, needed for regtech development.

The regtech market is a niche market. For their development, regtech solutions need inputs from two, usually separated, groups: technology developers and regulatory experts. When these communities are unaware of each other's insights, regtech solutions are unlikely to be developed. Industry associations are issues focused. Technology firms are product focused. The combined knowledge base of these various entities should be harnessed to solve the most pressing challenges.

A coordinated effort or platform bringing together stakeholders such as regulatory experts and regulators; technology and software developers; FIs; and entrepreneurs willing to invest and start new businesses, with the goal of regularly discussing specific pressing and emerging challenges, areas for collaboration, solutions and potential partnerships, and identify potential standards would enhance the entire community. This would also enable FIs to better understand the products offered by different emerging regtech competitors, and for interested participants from all disciplines to get to know each other and understand their different perspectives. In light of promoting competition in the financial services industry, platforms might best focus on open-source regtech approaches.

4. Barriers to knowledge sharing between regulators and financial institutions

Discussing bottlenecks in compliance with regulators can be legally difficult for Fis, impeding effective knowledge sharing between Fis, regulators and regtech ventures. Effective knowledge sharing in the community could benefit from regulators taking an active role in this space.

Regulators could set up a regulatory/supervisory knowledge hub to share knowledge on regulation, supervisory practice, and data formats and requirements with regtech developers. Building regtech solutions requires detailed knowledge of the regulatory architecture.

Equally, regulators could work to enable a "safe" environment for dialogue between the industry and its supervisors, in which firms would feel comfortable sharing information about compliance challenges and difficulties in a way that is not detrimental to their relationships with compliance and enforcement authorities and respects their commercial status as competitors. This can be done through a number of means:

a. Establishing clear rules of engagement, such as the Chatham House Rule, and general rules for usage of information as the UK AML authorities have done in their sphere,

b. Public statements by senior enforcement officials, utilizing global standard setters (BIS, EU, FSB, IAIS),

c. Proactive implementation of the "sandbox" approach that the FCA has been discussing, in which FIs can test new technologies in compliance and reporting in a controlled environment without risk of non-compliance for technical reasons.

Questions or comments regarding this publication may be addressed to:

Kristen Silverberg
Managing Director
Innovation
ksilverberg@iif.com

Andrés Portilla
Managing Director
Regulatory Affairs
aportilla@iif.com

Conan French
Senior Technology Advisor
Innovation
cfrench@iif.com

Bart van Liebergen
Associate Policy Advisor
Regulatory Affairs
bvanliebergen@iif.com

Stephanie Van Den Berg
Program Associate
Innovation
svandenberg@iif.com