Combatting Operational Risk through Regulatory Technology

Kateri Ganpat and Narissa Harrypersad[1]

Abstract

Global interest in regulatory technology, or RegTech, has grown rapidly within recent years following more demanding reporting requirements spurred by the Global Financial Crisis. In response, institutions and regulators alike have explored ways in which technological advancements can be used to their advantage, particularly in improving risk monitoring frameworks and counteracting operational risk associated with regulatory compliance and evolving financial innovation. In an effort to take stock of trends in the global regulatory sphere, this paper explores the development of RegTech internationally and analyses the opportunities and challenges of integrating advanced RegTech solutions to combat operational risk in Trinidad and Tobago.

JEL Classification Numbers: G21, G28, G32, O32, O33.

Keywords: compliance, financial regulation, fintech, innovation, regtech, operational risk.

September 2018

---

[1] The authors are research economists at the Central Bank of Trinidad and Tobago. The views expressed in the paper are those of the authors and not necessarily the views of the Central Bank.

1.0   INTRODUCTION

The number, frequency and complexity of regulatory demands for financial institutions have multiplied in the aftermath of the Global Financial Crisis (GFC). As such, institutions have been exploring cost-effective solutions to ease the burden of supervisory requirements and minimize operational risk stemming from non-compliance[2]. At the same time, the financial sector has embraced the ongoing technological revolution which has facilitated the integration of financial technology (FinTech) into business processes. While potential benefits of FinTech are many, it has introduced new avenues for operational risk in the financial system due to its evolution in the digital space.

Regulatory technology (RegTech) is a solution which capitalizes on the innovation driving FinTech and applies it to an organization's risk monitoring and compliance functions to improve the efficiency with which it executes its risk management framework. RegTech can be used by financial institutions to advance the automation and streamlining of data collection and analysis, which feeds into the production of analytical or actionable reports. Surveys conducted in 2018 list the top operational risk challenges of the global financial industry as the volume and pace of regulatory change and the ability to implement said changes (English and Hammond 2018). Further, information technology (IT) disruptions (from cyber-attacks or outdated systems), other forms of cyber risk, as well as model risk, rank alongside regulation as major operational risk concerns in the short term (Marlin 2018). RegTech solutions may serve as useful tools to address these issues within financial institutions.

Likewise, supervisors can harness the power of RegTech to improve the speed and quality of analytics, as well as address the gaps in supervision due to the influx of new data and information required by the changing financial and regulatory environment. RegTech supports communication across an independent, digitized platform thus improving regulatory reporting and offering regulators the ability to directly access institution data. In this way, supervisors will be able to conduct an unbiased analysis of company data and flag issues in real-time, thus reducing resolution time for identified threats to financial stability through

---

[2] Operational risk is defined as the risk of losses resulting from deficiencies in internal processes, people and systems, or from external factors and events (Basel Committee on Banking Supervision 2011). Compliance risk can form part of an organization's operational risk function and is defined as "the risk of legal or regulatory sanctions, material financial loss, or loss to reputation…as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its activities" (Basel Committee on Banking Supervision 2005).

operational risk. The wealth of data available can also be simplified and structured in user-friendly interfaces to inform forward-looking policy decision-making (Arner, Barberis and Buckley 2016).

This paper aims to introduce the concept of RegTech, in particular its potential contribution to domestic operational risk management from an institutional as well as a supervisory[3] perspective. While some aspects of the institutional assessment can be generalized for the financial industry as a whole, the paper focuses on the banking system given their size in the domestic financial system[4]. The selection of case studies which demonstrate the use of RegTech by banks or supervisory bodies is fairly limited. In this regard, Section 2 provides a background of RegTech development; Section 3 explores the evolution of the local regulatory and reporting framework and the possible repercussions faced by banks; Section 4 discusses considerations surrounding the implementation of advanced RegTech solutions on domestic activities; and Section 5 concludes.

2.0   BACKGROUND

2.1   Development of RegTech

The GFC revealed weaknesses in the regulation of the financial system and the avenues through which financial companies were able to exploit loopholes in existing rules and contribute to the build-up of systemic risk[5]. In response, international standard-setting bodies and market supervisors have issued guidance and legislation that have materially changed the way in which financial institutions design and implement their risk management frameworks. By 2015, the total number of regulatory changes since the GFC, including publications and announcements, had increased by an estimated 492 per cent (Hugé, Duprel and Pescatore 2017). Among other things, the new rules were intended to mitigate the risks of complex products that developed pre-crisis, which were heightened by the expansion of cross-border financial conglomerates in the absence of consolidated supervision. In order to improve transparency and

---

[3] RegTech utilized in the supervisory capacity is also referred to as "SupTech".
[4] The consolidated banking system of Trinidad and Tobago accounted for approximately 46 per cent of financial system assets as of December 2017 (CBTT 2018).
[5] Some bank holding companies took advantage of regulatory inconsistencies between banks and their non-banking subsidiaries including: the differences in capital requirements; recognition of and provision for loan losses; as well as consumer compliance regulations that ensured borrower creditworthiness (Demyanyk and Loutskina 2014).

aid in monitoring the accumulation of risk in the macro-financial environment, regulators have exponentially increased their demands with respect to the frequency and granularity of institutional data.

These developments have proven to be a challenge for both regulators and financial institutions whose IT systems have not been well-equipped to handle the volume and complexity of regulatory changes in the rapidly evolving financial environment. Legacy systems that have been developed pre-crisis are characteristically costly to maintain, difficult and expensive to modify, prone to crashes and susceptible to cyber-attacks (Armstrong 2017). Given the pace and scale of regulatory reform, increased time, managerial attention and human and capital resources are therefore necessary to ensure institutions are not at risk of substantial fines for breaching regulation and failing to implement adequate controls. Given potentially compounding operational expenses, the need for a more sustainable, cost-efficient solution is evident.

More recently, the financial system has benefitted from innovations such as artificial intelligence, distributed ledger technology, mobile access and cryptography. These and other technologies have enabled the digitization and automation of new and traditional products and services in the financial sector, that have lowered transaction costs, supported financial inclusion, increased competition and improved the efficiency of banking processes (Basel Committee on Banking Supervision 2018). However, the spread of FinTech companies and the transformation of financial services have presented new risks including cyber risks, interconnectedness and concentration risk (He, et al. 2017, Basel Committee on Banking Supervision 2018). Three major forms of cyber risk exist – business disruptions, fraud and data security breaches. While business disruptions and fraud can lead to direct financial losses, all forms can affect an institution's bottom line through its impact on reputation and associated legal costs (Bouveret 2018).

The reluctance to upgrade functionally inefficient systems has placed some firms at a competitive disadvantage as they are not able to maximize the benefits of technological innovation being adopted by peers in the industry. Regulators are also challenged with the pressure of upgrading IT infrastructure in order to process the large and complex datasets being requested of the institutions, as well as the unique digital data introduced by these FinTech products and services. RegTech therefore has emerged as an opportunity for regulators and financial institutions to overcome these challenges by addressing operational risks related to veracity of data and information; antiquated processing systems; business disruptions; information security breaches; and overall regulatory compliance.

2.2 RegTech Solutions Offered by Third-party Service Providers

In recent years, there has been an acceleration in the growth of companies that offer innovative solutions for compliance and regulation as the popularity and application of FinTech has expanded. These include small start-ups as well as globally recognized consulting companies which tend to specialize by: solution(s) offered; sector in the financial system; and institution- or regulator-focus. In the past, new regulation typically resulted in the costly, time-consuming development of an appendage to legacy systems, which had to be adapted to remain in sync with existing IT infrastructure (Hugé 2018). These traditional systems currently dominate the compliance space. RegTech firms can provide independent, agile alternatives that are able to keep up with the pace of regulatory changes while reducing physical and operational costs of amendments.

The solutions offered by RegTech companies, as well as the various technologies supporting their implementation, have been categorized in Figure 1.

Figure 1: RegTech Solutions and Enabling Technologies

Source: Categorization based on Hugé, Duprel and Pescatore (2017).

Table 1 provides a brief overview of the specific innovations that underlie RegTech solutions.

Table 1: Enabling Technologies

TECHNOLOGY	DESCRIPTION
Cloud Computing/ Cloud-based Services/ Hosted Solutions	Cloud computing, also called cloud based services or hosted solutions, utilizes remote servers hosted over the internet to maintain, process, share and back-up stored data.
Application Program Interface (API)	API refers to the suite of rules and standards that define how different software communicate and interact with each other.
Big Data Analytics	Big data analytics refers to the real-time organization and mining of large volumes of structured and unstructured data to unearth correlations and trends.
Artificial Intelligence (AI)	AI is the science which utilizes computers to make automated decisions, predictions and recommendations informed by insight garnered through the analysis of big data.
Machine Learning	Machine learning is the subset of AI that enables computers to continuously analyse and learn from trends observed in reported data, without the need for specific programming to define the new learning.
Distributed Ledger Technology (DLT)	DLT refers to the platform that allows a database to be replicated, shared and synchronized across a network of multiple parties, creating a permanent digital record of any mutually-agreed upon transaction. The term DLT is often used synonymously with blockchain, although the blockchain is one type of distributed ledger.
Biometric Technologies	Biometric technologies facilitate the automated authentication of a client by validating distinctive characteristics that have previously been captured and stored digitally.

Source: (He, et al. 2017, Institute of International Finance 2015, Mills, et al. 2016, Toronto Centre 2017).

Accordingly, the issues that can be addressed by RegTech solutions are described as follows:

2.2.1   Regulatory Reporting

- The growing volume and granularity of data expected by licensees, and the transference and storage of large files have become an issue. Problems manifest particularly when data is requested and collected in a form that mimics paper reports, despite being shared electronically (Institute of International Finance 2016). Manual completion and processing of regulatory returns is more likely to be time consuming and prone to human error.

- Regulatory reporting solutions focus on the automation of data sharing through the use of **API** and **cloud computing**, where regulators can access data and information in a structured, simplified format on a centralized server. This could assist the audit process by allowing the review of real-time transaction data to enhance monitoring and auditing. In contrast, **DLT** offers a decentralized solution where data and information can be shared quickly and accurately on a secure blockchain. Both innovations organize data in a format that enables the application of **big data analytics** to produce standard and ad hoc reports as desired by the regulator. This process can reduce the overall costs involved in sharing information with the regulator, thus increasing efficiency and reducing the cost of compliance.

2.2.2   Risk Management

- Post-GFC regulation such as Basel III stipulates capital and liquidity requirements that can be estimated by standardized methods or internal modelling. Stress testing and scenario analysis[6], expected loss provisioning[7] as well as other types of risk modelling depend on large amounts of aggregated risk data (both historical and forward-looking) to understand and improve forecasts of future threats. Additionally, more stringent requirements in place for Global Systemically Important Banks underscore the need for effective risk data aggregation and reporting (Basel Committee on Banking Supervision 2013).

- Risk management solutions enable the automation and simplification of risk data in a well-organized database to compute, inter alia, current exposure levels, capital, asset quality and

---

[6] As expected under Pillar II of the Basel III capital requirements.
[7] As defined in the International Accounting Standard Board's *IFRS 9 Financial Instruments* requirements.

liquidity ratios. **AI** and **machine learning** can be utilized to detect and assess risks of non-compliance to identify threats in advance and encourage corrective action. In particular, modelling components can hinge on **big data analytics** by applying intense computing power to the data available.

2.2.3 Transaction Monitoring

- Know your customer (KYC) regulations refer to the set of rules that require financial institutions to collect and analyse customer or counterparty data to aid in the detection and prevention of, inter alia, fraud, money laundering and terrorism financing. KYC processes should continuously monitor regular transactions so that suspicious activity will be flagged, as well as assess the level of risk posed by the counterparty through exposures to known individuals (for example, politically exposed persons).

- The decentralized database created by **DLT** makes KYC processes more efficient by storing immutable transaction data that can be updated by institutional members of the blockchain, thus establishing a permanent financial record. **AI** and **machine learning** can be applied to this transactional data to interpret patterns in customer behaviour and flag, prevent or report suspected illegal activity in real time. Reporting this information forms a key component of compliance with Anti-Money Laundering (AML) and Combatting the Financing of Terrorism (CFT) regulations.

2.2.4 Identity Management and Control

- Counterparty due diligence and KYC tasks, as required by AML/CFT regulations, can be manual and repetitive in nature and therefore not efficient or economical. The issue has come to the fore in light of correspondent banking relationships as institutions could benefit from the ability to leverage KYC performed by other organizations (Institute of International Finance 2016).

- Identity management and control tools can hinge off of **DLT** by storing all KYC information in a secure database, creating a digital identity for a customer or counterparty which can be accessed in a timely and cost-efficient manner for identity checks. By storing due diligence data in a decentralized location, financial institutions that have agreed to participate in the blockchain can immediately access and transparently update KYC data on shared customers

and counterparties. **Biometric technologies** can also support blockchain identity control by enabling digital identification through techniques such as fingerprint scanning and facial recognition. Further, **AI, machine learning** and **big data analytics** can be applied to analyse the existing database and produce ad hoc reports on specific customers or type of customer by risk exposure to aid the risk management function.

2.2.5 Compliance

- The compliance function involves regulatory watches which keep track of relevant upcoming regulation; compliance project management which defines the tasks and resources necessary to comply with new regulation within a stipulated timeline; regular compliance health checks; and cyber security and due diligence (Hugé, Duprel and Pescatore 2017). These tasks can become very complex as they require input and coordination of several areas of an organisation.

- Compliance solutions offer improved, real-time regulatory watch based on **AI** which automates the interpretation of regulation. This aids in continuous compliance health check and makes it easier for institutions to keep up with the pace of regulatory changes.

2.3   Growth of RegTech Internationally

While some organisations have long applied a rudimentary form of RegTech in their business, attention was traditionally placed on the digitization of the regulatory reporting and compliance functions (Arner, Barberis and Buckley 2016). It has been estimated that over 300 RegTech companies were established up to 2016 but Figures 2 and 3 show that there has been tremendous growth since then, particularly in non-traditional RegTech solutions provided by start-up companies (Alvarez & Marsal and Burnmark 2018).

Figure 2: Share of RegTech Startups by Solution[8], 2017

Figure 3: Growth in Number of RegTech Startups by Solution, 2015 - 2017
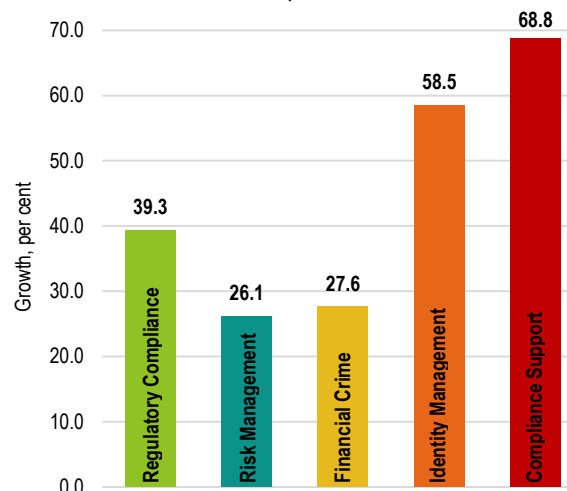
Source: (Alvarez & Marsal and Burnmark 2018).

This reflects the objective of newer RegTech solutions to move from a concept of 'big data' to 'smart data', by leveraging modern technologies (Ivanoski, et al. 2017). There appears to be strong global interest in harnessing RegTech in the short term as evidenced by the 102 per cent growth[9] in funding to the sector for the year ended March 2016 (Transatlantic Policy Working Group Fintech 2017). Additionally, the *2016 Global CEO Outlook Study* (KPMG International 2016) stated that CEOs believed economic conditions and

---

[8] Regulatory compliance refers to "offerings that help banks in gathering regulatory intelligence, mapping policies, compliance governance and automated data sharing with regulatory authorities" and financial crime refers to "offerings that help banks monitor financial transactions in real-time to detect fraud, market abuse, money-laundering or terrorist financing activities" (Alvarez & Marsal and Burnmark 2018). These are comparable to this paper's categorizations of Regulatory Reporting and Transaction Monitoring, respectively.

[9] This represents investments of US$238 million across 34 deals.

technology would be the major contributors to the growth of their company. The *Cost of Compliance 2018*[10] survey report (English and Hammond 2018) supported this view by adding that 61 per cent of firms surveyed anticipated an increase in their compliance budgets for 2018[11] to address, inter alia, investment in compliance monitoring tools and activities; automation of old systems to improve efficiency in data reporting and analysis; outsourcing of specific services; and additional skilled and senior resources.

Despite this, adoption of RegTech solutions to date is still in its nascent stages due to a number of limitations including institutions' uncertainty over the regulatory stance and credibility of untested technologies (Financial Conduct Authority 2016). As such, there has been the introduction of "regulatory sandboxes" for RegTech and FinTech where institutions are encouraged to experiment with new innovative technologies in a controlled environment. Regulatory sandboxes have been established in jurisdictions such as the United Kingdom, Australia, Singapore, China and Hong Kong (Baxter 2016).

The attention placed on technological innovation in more developed countries is reflected in the global distribution of RegTech firms at the end of March 2017 (Figure 4). Developing countries, such as those in the Caribbean and the "rest of the world", have been slower to adopt as advances in technology and its application to the financial services sector have lagged behind.

Figure 4: Global RegTech Companies by Location, March 2017
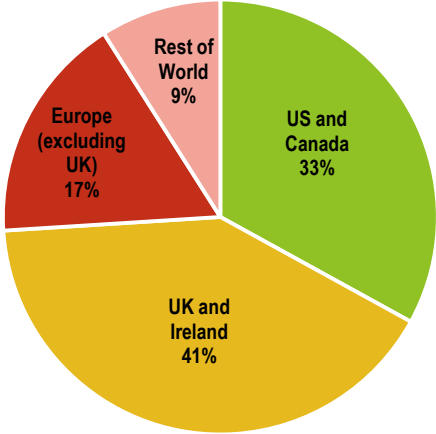
Source: Illuminate Financial Management.

---

[10] Thomson Reuters Regulatory Intelligence conducted its ninth annual cost of compliance survey in Q1 2018. Over 800 responses were received from members of the financial services industry, including asset management, insurance, banking and investment, from areas such as Asia, Australasia, Canada, Europe, Middle East, United Kingdom and the United States.
[11] A mere 6 per cent expected costs to reduce.

2.4   SWOT Analysis of RegTech Solutions

RegTech solutions provide a range of opportunities for financial institutions and regulators. However, as with any innovation, there are potential vulnerabilities. Table 1 presents the strengths, opportunities, weaknesses and threats associated with RegTech.

Table 1 - SWOT Analysis

STRENGTHS	WEAKNESSES
• Reduce the cost of compliance in terms of human resources and the avoidance of fines. • Cloud-based design facilitates easy, quick and secure sharing of data. • Real-time insight through continuously collecting and monitoring data.	• Online presence increases vulnerability to cyber-attacks. • Depending on the scenario, human judgement may still be required to make appropriate decisions.
OPPORTUNITIES	**THREATS**
• Improved KYC through improved customer identification and authentication. • Greater efficiency for AML/CFT policy through the use of AI to monitor vast amount of data. • Integrate regulatory reporting requirements and fully automate reporting. • Facilitates compliance project management through the use of tools which could aid in the planning and tracking of upcoming regulations. • Improve risk data reporting capabilities.	• Impact of cyber risk is potentially more severe/widespread. • Misleading results if there is erroneously inputted data. • Using RegTech solutions without fully understanding the downsides can potentially increase susceptibility to unknown/unidentified risk. • Concentration risk if multiple organisations utilize the same RegTech service provider.

Sources: (Bauguess 2017, Basel Committee on Banking Supervision 2018, Liebergen and Ekberg 2017, He, et al. 2017, Hugé, Duprel and Pescatore 2017, Arner, Barberis and Buckley 2016, Toronto Centre 2017).

3.0   LOCAL REGULATORY AND REPORTING FRAMEWORK

3.1   The Central Bank's Experience with Technology in Supervision

3.1.1 Data Collection and Processing

While the Central Bank of Trinidad and Tobago (the Central Bank) has not yet adopted any of the advanced RegTech solutions discussed, the way in which it has utilized technology to facilitate banking supervision has progressed over the years. Initially, the Central Bank relied solely on physical submissions of regulatory forms from the financial institutions on a periodic basis, as mandated by the Financial Institutions Act, 2008 (FIA). Upon receipt, data entry operators in the Financial Institutions Supervision Department (FISD) and Research Department were responsible for entering the data onto a single mainframe. There was no distributed computer system in place at the time and therefore, subsequent to data input, the IT Department was responsible for centrally processing the data. They then generated reports to be forwarded to relevant units or other departments.

The Central Bank began to embrace technological development and the use of personal computers was adopted resulting in a change in operations. Data entry operators were now responsible for entering information received from physical submissions into a Microsoft Excel template for further analysis. In addition, Microsoft Access was utilized for the storage and review of relational data, for example, to generate reports related to timeliness of submissions.

The reliance on Microsoft Excel however resulted in numerous data control errors. For example, multiple versions of the same document would have existed after updates were made by one individual but not communicated to all persons with access to the document. In addition, Microsoft Access was deficient in its ability to easily generate time-series reports as it was limited to creating cross-sectional reports only. As such, the benefits of having a centralised system for data warehousing which could also be used for time-series analysis became increasingly evident. This led the Central Bank to consider available software which could facilitate this process.

In 1994, coinciding with the revision of the regulatory forms, a decision was taken by the Central Bank to utilize new software to assist in its data processing function. The Forecasting Analysis and Modeling Environment (FAME) software was adopted in 1995 to automate some aspects of the process to a greater

extent. However, while this system facilitated easier aggregation of data, the Central Bank still relied on physical submissions by the financial institutions for some time.

At present, reporting institutions are required to submit hard (physical) and soft (using Microsoft Excel) copies of relevant forms to the Statistics Department of the Central Bank. Completed soft copies are encrypted and submitted via electronic mail. The Statistics Department is then tasked with the responsibility of verifying the data received and uses the FAME software to facilitate this process. Although software applications are utilized, it can still be a time-consuming and human resource intensive process since persons are usually heavily involved with performing checks and balances on data that may have to be addressed and resubmitted. Further, the deadline for submitting different regulatory may differ (for example, 10, 15, or 20 working days after the end of the month) adding to the effort needed to keep track of adherence to stipulated deadlines.

3.1.2 Monitoring Banks' Compliance

In the past, the rules-based or compliance-based approach to supervision was applied and placed emphasis strictly on breaches in compliance and the legal consequences for the institution. A more pro-active approach to supervision has developed internationally which focuses also on the inherent risks within an institution due to their financial positions, cross-border activities, business models and management practices. The FISD applies this risk-based supervisory framework, comprising on-site examinations, off-site monitoring and ad hoc analyses to assess the continued safety and soundness of licensees.

With respect to the banking system, that is, the commercial banks and non-banking financial institutions, on-site examinations take the form of meetings with designated representatives. Several matters are discussed, including: reports on institutional practices; progress with meeting governing standards; performance of the institutions; and future plans of the institution. These are performed on a routine basis whereas ad hoc analyses are unplanned interventions which may take place as and when required.

Off-site examinations depend heavily on the data aggregated by the Statistics Department. The FISD peruses the data using Microsoft Excel to review trends and identify anomalies by comparing information received with benchmarks. Further, the FISD is responsible for reviewing minutes of the Boards of Directors of the banks to monitor governance practices as well as ensure they remain compliant by upholding the mandates set out by the FIA. This process is inevitably human resource intensive since there is no automated method for highlighting particular items that may trigger risk.

While the primary focus of the FISD is micro-prudential supervision, that is, promoting the stability of each of its licensees by assessing idiosyncratic risks, it is complemented by a macro-prudential approach. Macro-prudential supervision aims to limit systemic risk within the financial system whereby stress emanating from a component of the financial or real sector threatens the health of the financial system as a whole, with negative feedback effects for the real economy. The macro-prudential analysis function lies primarily within the Research Department which monitors vulnerabilities and risks to financial system stability through routine analysis of financial soundness and early warning indicators, as well as internal stress testing. This is performed in the context of developments within the financial or real sector, which are actively monitored to determine the potential to trigger systemic risk.

3.2 Impact of New and Amended Standards on Banks' Cost of Compliance

Regulation in the local financial landscape is driven by standards set by international bodies. For example, the Central Bank is heavily guided by changes in the Basel Framework as outlined by the Basel Committee on Banking Supervision (BCBS) as well as the International Financial Reporting Standards (IFRS) developed by the International Accounting Standards Board (IASB). Other applicable developments include the Tax Information and Exchange Agreements (United States of America (US)) Act (TIEAA) under which the Financial Account Tax Compliance Act (FATCA) is covered, as well as updated guidelines set by the Financial Action Task Force (FATF) on AML/CFT.

3.2.1 The Basel Framework

The Basel Framework is one of the main guiding principles used by the Central Bank in its oversight of banking licensees. Basel guidelines are meant to serve as basic minimum standards which should be employed in order to minimize the development of credit, market and operational risk and outlines measures which should be adopted by banks and supervisory authorities to restrain growth of such risks. The initial set of principles issued by the BCBS in 1988, known as Basel I, has been revised over time to close regulatory gaps. This included the issuance of Basel II in 2004, as well as the latest iteration, Basel III, which was intended to enhance and supplement Basel II to address issues observed in the GFC.

Locally however, banks continue to be assessed on Basel I principles while plans are underway for the formal implementation of Basel II standards and some elements of Basel III. [12] The proposed changes to the supervisory framework under this new model would require that banks pay greater attention to the risk monitoring and reporting processes given the introduction of an additional charge for operational and other risks not captured under Basel I. Adherence to updated standards stipulates that banks take measures to identify and manage potential risk; promote enhanced data reporting and aggregation; and ensure disclosures are in line with updated standards. These proposals would undoubtedly impact banks' modus operandi, and it is expected that additional human and infrastructural (IT) resources will be necessary to aid in compliance.

3.2.2   Foreign Account Tax Compliance Act[13]

FATCA is legislation aimed at combatting tax evasion by citizens of the US who hold offshore accounts. The law requires financial institutions to enter into an agreement with the US Internal Revenue Service (IRS), the TIEAA, in order to disclose information related to account-holders who are US citizens.[14]

The principal impact of FATCA legislation on the cost of compliance is through the cost of updates to procedures to ensure that all relevant information is obtained from customers and further, ensuring consumer data is stored in a central location (Bandyopadhyay 2014). This is intended to support due diligence in terms of KYC data collection, customer identification and reporting, both in terms of new and existing accounts. Given the repercussions for non-compliance with FATCA[15] and the threat to correspondent banking relationships with the US, local institutions would have been compelled to make adjustments to adhere to these guidelines. At the same time, the supervisory process would have been adjusted to consider these new requirements.

3.2.3   International Financial Reporting Standards

The International Financial Reporting Standards (IFRS) are a set of standardized accounting principles developed by International Accounting Standards Board (IASB) which are used to guide accounting practices and reporting globally. Similar to the evolution of the Basel standards, accounting standards have

---

[12] See *Proposals for the Implementation of Basel II/III for Institutions Licensed under the Financial Institutions Act, 2008 Phase I,* December 2014.
[13] (Internal Revenue Service 2018)and (Bandyopadhyay 2014).
[14] The law also requires "Non-Financial Foreign Entities to disclose the identity of their US owners to the IRS."
[15] In the form of a 30 per cent withholding tax on US denominated transactions.

advanced over time to address transforming risk. Following the GFC, a significant change was made to the way credit risk should be modelled in the new IFRS 9 standard. In particular, an expected credit loss impairment model, in which banks would be required to recognize an impairment provision before a loss event actually occurred, was recommended to replace the incurred loss model previously employed (Deloitte 2016).

IFRS 9 became mandatory for companies for annual reporting periods beginning on or after January 1, 2018. Locally, the transition to IFRS 9 is not yet complete but would require firms to make a number of adjustments to current practices. The new Standard will necessitate changes to systems and processes (PricewaterhouseCoopers 2017) which will enable the collection of relevant data to calculate expected losses. However, banks may face modelling risk resulting in incorrect estimations due to over-complication or misspecification of the expected credit loss model. There may be additional concerns with respect to availability of resources and limitations of, and integration with, the current IT systems.

3.2.4   FATF Guidelines on Anti-Money Laundering/Combatting the Financing of Tourism

The FATF is an inter-governmental body which sets standards and proposes appropriate guidelines to aid in combatting money laundering (ML) and terrorist financing (TF). In order to assess the adherence to guidelines, the FATF conducts periodical reviews of member countries to determine whether sufficient measures have been taken by governments and financial institutions to ensure compliance.

From the financial institutions' perspective, and similar to requirements to adhere to stipulations under the FATCA, customer due diligence is also important to ensure compliance with FATF Recommendations. The most recent FATF Mutual Evaluation Report for Trinidad and Tobago conducted in 2016 noted that the country suffered from a range of deficiencies with respect to compliance. Many of the gaps identified stemmed from the actions (or inaction) of the authorities responsible for ML and TF, for example, the National AML/CFT Committee and the Financial Intelligence Unit of Trinidad and Tobago. However, it was highlighted that financial institutions were considered to have a low compliance in the area of customer due diligence. Notably however, local banks have been keen on adopting measures to better identify and track clients, as well as take measures against ML and TF risks by investing in infrastructure to aid in ensuring compliance with recommendations.

4.0   OPPORTUNITIES AND CHALLENGES

In the context of the changing financial landscape and the availability of newer technologies, current approaches to supervision and risk management in Trinidad and Tobago may be inadequate and would benefit from the introduction of modernized RegTech solutions. The same toolset is available to both regulators and licensees; however, their particular objectives dictate RegTech application within their organisations. It must be underscored that RegTech companies are third-party service providers and are not ultimately responsible for ensuring an institution remains compliant or executes sound risk management strategies (Armstrong 2017). Rather, they are technology companies limited to the functions predefined within their systems. It is therefore pertinent that users of the systems – regulators and licensees alike – be au courant with the application of relevant solutions as well as interpretation of their output as it relates to informing forward-looking policymaking and risk management decisions.

4.1   The Effect of RegTech on Regulators' Job Specifications

RegTech is seen as complementary to the role of the regulator, rather than a replacement. While some solutions may automate specific regulatory functions, expert judgement based on trends and experiences will remain a vital part of forward-looking policymaking. RegTech has the potential to impact several regulatory responsibilities including, but not limited to, the statistics function, financial institution supervision and macro-prudential supervision.

4.1.1   Statistics

- The traditional use of templates issued to licensees for data collection (see Section 3.1) limits flexibility in data manipulation, increases the likelihood of inconsistencies across different reporting templates (as well as individual versus aggregate system data) and can hinder efficient data aggregation as required by post-crisis regulatory reform (Toronto Centre 2017). Further, if additional data were desired, it could only be achieved through a costly amendment to the relevant systems; this may draw objection from licensees.

- The regulatory reporting solution may be of most value to the statistician. This can support the collection of a vast amount of granular data, which can be verified, manipulated and analysed. Employees would no longer be required to manually verify data quality, thus reducing processing

time and the likelihood of human error. Instead, the focus would be on extracting unique data sets from the wealth of information in order to report on emerging trends.

4.1.2   Financial Institution Supervision

- On-site visits conducted by the supervisor serve to complement intelligence gathered from regular reporting and allows the supervisor the opportunity to conduct a more thorough investigation into possible deficiencies observed through off-site analysis of submitted data and information. However, data reporting is typically lagged and a complete picture may not be available due to inconsistent frequencies with which different reports are required. This delays supervisory action in addressing heightened vulnerabilities.

- RegTech analytics can be used as an input to the supervisory risk-based approach, leveraging the regulatory reporting, risk management and compliance solutions. These can be used to produce comprehensive risk profiles, including key performance indicators for individual institutions, based on readily available and up-to-date data. Supervisors can have real-time access to data and transactions which aids in timely identification or notification of breaches in compliance and other areas where supervisory attention may be most necessary for early intervention.

4.1.3   Macro-prudential Supervision

- Macro-prudential supervision takes a broader approach to financial supervision and seeks to pinpoint areas that pose systemic risk to the entire financial sector or the wider economy. As with the current approach to financial institution supervision, supervisory action can be delayed posing a risk to financial stability.

- RegTech can provide structure to large amounts of data, both internal and external (even outside of the financial system), to extract useful information on developments within the real or financial sector that can impact financial soundness indicators. Forward-looking supervision will leverage more efficient data collection and RegTech analytics to direct supervisory resources as necessary.

4.2 The Effect of RegTech on the Relationship between the Regulator and its Licensees

Following from above, RegTech can positively impact the type of interaction observed between the Bank and regulated institutions through enhancing various components of the supervisory process. For example,

- **Increased Collaboration and Communication –** Employment of RegTech to the reporting process would result in greater collaboration and communication between the Central Bank and its licensees. Regulatory changes and updates may be plentiful and potentially daunting to licensees which are tasked with the responsibility of understanding exactly what is required of them and subsequently taking measures to ensure that requirements are met. RegTech can aid in the communication process since it would involve standardization of data and clarity in terms of what exactly would be collected and for what purpose. Further opportunities exist in terms of the application of machine-readable regulation which proposes the standardization of regulatory requirements in a manner that would allow RegTech solutions to automatically address additional requests made by the regulator (Butler, North and Palmer 2018).

- **Facilitate Transparency and Trust among Parties –** Advanced RegTech techniques could facilitate the real-time observation of data and allow for corrective action to be taken rapidly if needed, and with greater transparency, engendering trust among all parties involved. As a direct result of the extensive detail required to adhere to increased regulatory demands, RegTech could improve the accuracy of reporting by financial institutions as well as the Central Bank's ability to process, interpret and report on the information received.

- **Enhanced Reporting –** RegTech could further enhance exchange of information relating to KYC requirements among parties, given increased efficiencies in the due diligence process which could be facilitated through enhanced data collection, storage and streamlining of information related to customers. Digital identities associated with customers could also enhance banks' ability to identify and flag suspicious activity. With established agreement between the parties, the Central Bank can capitalize on this database using DLT to perform necessary checks and balances.

4.3 Challenges to Adoption and Implementation

Long-run gains in efficiency resulting from changes in the modus operandi of different stakeholders are expected to offset direct expenses brought on by the acquisition of RegTech solutions through a third-party service provider. However, the magnitude of these and other associated costs must be thoroughly assessed. Beyond direct budgetary constraints, other challenges to adoption and implementation exist and must be considered in evaluating the feasibility of RegTech introduction. These include:

- **Conversion of legacy systems –** Traditional legacy systems are based on complex architecture and may have been designed to record data in a limited format. They typically do not have the capacity to capture the volume, granularity or cross-section of data required to apply RegTech solutions hinged on AI or big data analytics. Upgrades to existing architecture can be considered short-term fixes. Investment must be made in conversion to software-based infrastructure to, inter alia, manage big data or construct relational databases in the digital space.

- **Investment in human resources –** In the short term, RegTech introduction can mean increased expenses in training existing staff (including management) in the correct usage of the systems and interpretation of the output. It may also require investment in new employees who have the requisite working knowledge of the innovative technologies and the skillset to combat associated risks. In the long-run, RegTech solutions may result in a reduction in staff or a realignment of responsibilities that rely on expert judgement.

- **Risk averse culture/ Uncertainty over regulation –** Globally, there has been hesitation surrounding innovation, particularly for newer solutions which do not yet have a proven track record. Management, particularly those without the technological expertise, may be more risk averse and prefer to invest in upgrading legacy systems rather than 'experiment' with technology-based solutions. For financial institutions, this uncertainty is compounded by doubts surrounding supervisory approvals, making engagement with RegTech firms risky.

- **Third-party risk –** A disruption or deterioration in the quality of services provided by the RegTech firm can result in a direct operational cost to the institution, which bears ultimate responsibility for regulatory compliance. Further, concentration risk exists if several institutions and/or the regulator share the same service provider. Disruptions in this scenario can have systemic implications.

- **Cyber Security –** Movement to software-based infrastructure increases vulnerability to cyber-attacks that can disrupt service as well as expose sensitive customer or institution data. Weaknesses in cyber security can also give way to theft as well as integrity issues such as fraud. These can generate significant operational losses and compromise the reputation of affected institutions.

The expected benefits to be gained from the introduction of RegTech solutions warrant further investigation to determine the ways in which these challenges may be overcome or minimized within a financial institution or regulatory authority. This may mean a strategic adjustment to long-term planning within the organizations and greater collaboration among stakeholders, including regulators; financial institutions; RegTech service providers; academia; and other players in the market. Two-way communication is key to avoid misinterpretation of regulatory requirements.

5.0 CONCLUSION AND RECOMMENDATION

This paper aimed to introduce the concept of RegTech, whose popularity has been accelerating within the international financial services industry. It is evident that its introduction into the financial landscape can provide significant opportunities for operational risk management from an institutional perspective to ensure compliance with changing regulatory rules. While it is in its nascent stages in the global regulatory sphere, there exists tremendous potential for increased efficiency in routine operations and it can serve as a complementary tool, along with expert judgment, for effective supervision.

The local financial sector has embraced financial innovation. Institutions have reported enhancements to internal operations in a bid to increase digitization and it is evident that there is a desire to increase the efficiency of internal processes and facilitate the adherence to updated requirements. As such, the regulator must keep abreast of operational risks inherent in newer forms of technology and investigate the tools offered by RegTech to mitigate these risks. The regulator should also aim to encourage technological development and innovation, without compromising financial stability. Careful planning must go into the timing of new regulation lest it prematurely stymie growth.

Initiatives such as the "regulatory sandbox" have been a starting point in several jurisdictions to foster more practical understanding of the innovative technologies as it pertains to an institution's needs and business model. The regulator must remain cognizant of the risks in the selection of a service provider, both in terms of operational availability as well as confidentiality of data shared. These issues may surface through regulatory sandbox experiments which can provide greater insight into systemic risks that could manifest as a result of implementation. Results of sandbox initiatives can therefore guide conversations surrounding additional regulation which may be necessary to facilitate use of the solutions.

In order to support the activities required to ensure compliance by financial institutions, research should be extended to identify RegTech firms and the services they offer with respect to supervisory RegTech. Subsequently, a thorough feasibility assessment should be conducted for the Central Bank and consideration should be given to system interoperability between an individual institution and the regulator. In the meantime, the Central Bank continues to monitor regional and international developments in the RegTech space as it makes on-going strides in improving risk-based supervision for the promotion of financial stability.

Bibliography

Alexander, Kern. *Financial Inclusion, FinTech and RegTech.* Centre for Risk Studies, University of Cambridge, 2017.

Alvarez & Marsal and Burnmark. "RegTech 2.0." 2018.

Armstrong, Patrick. "The Adoption of RegTech within the Financial Services Industry: Ten years from the Start of the 'Great Financial Crisis'." *European Securities and Markets Authority.* May 2017. https://www.esma.europa.eu/sites/default/files/library/pka_speech_regtech.pdf (accessed January 2018).

Arner, Douglas W., Jànos Barberis, and Ross P. Buckley. *FinTech and RegTech in a Nutshell, and the Future in a Sandbox.* Research Foundation Briefs, CFA Institute Research Foundation, 2017.

Arner, Douglas W., Jànos Barberis, and Ross P. Buckley. "FinTech, RegTech and the Reconceptualization of Financial Regulation." *Northwestern Journal of International Law & Business, Forthcoming*, 2016.

Arner, Douglas W., Janos Nathan Barberis, and Ross P. Buckley. "The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data." *Journal of Financial Transformation 44*, 2016: 79-86.

Augur, Hannah. "RegTech: The 2016 Buzzword is Turning Heads." *Dataconomy.* 3 May 2016. http://dataconomy.com/2016/05/regtech-the-2016-buzzword-is-turning-heads/ (accessed January 19, 2018).

Bandyopadhyay, Subhasis. "Impact of FATCA on financial institutions ." *Mindtree.* 2014. https://www.mindtree.com/sites/default/files/2017-10/369_mindtree-thought-posts-white-paper-impact-of-fatca-on-financial-institutions.pdf (accessed June 2018).

Basel Committee on Banking Supervision. *Compliance and the compliance function in banks.* Bank for International Settlements, 2005.

Basel Committee on Banking Supervision. *Principles for effective risk data aggregation and risk reporting.* Bank for International Settlements, 2013.

Basel Committee on Banking Supervision. *Principles for the Sound Management of Operational Risk.* Bank for International Settlements, 2011.

Basel Committee on Banking Supervision. *Sound Practices: Implications of fintech developments for bank and bank supervisors.* Bank for international Settlements, 2018.

Bauguess, Scott W. *The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective.* 21 June 2017. https://www.sec.gov/news/speech/bauguess-big-data-ai.

Baxter, Lawrence G. "Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures." *Duke Law Journal Vol. 66*, 2016: 567-604 .

Bouveret, Antoine. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment.* Working Paper, International Monetary Fund, 2018.

Butler, Tom, Paul North, and John Palmer. *A New Paradigm for Regulatory Change and Compliance.* RegTech Council, 2018.

CBTT. *Financial Stability Report 2017.* Central Bank of Trinidad and Tobago, 2018.

Deloitte. "A Drain on Resources? The impact of IFRS 9 on Banking Sector Regulatory Capital." 2016.

Deloitte. *RegTech is the new FinTech. How agile regulatory technology is helping firms better understand and manage risks .* Deloitte, 2017.

Demyanyk, Yuliya, and Elena Loutskina. *A Gap in Regulation and the Looser Lending Standards that Followed.* Economic Commentary, Federal Reserve Bank of Cleveland, 2014.

Eldridge, Paul W. *The FATCA Challenge Facing Caribbean Banks.* PricewaterhouseCoopers Bermuda, 2012.

English, Stacey, and Susannah Hammond. *Cost of Compliance 2017.* Thomson Reuters, 2017.

English, Stacey, and Susannah Hammond. *Cost of Compliance 2018.* Thomson Reuters, 2018.

English, Stacey, and Susannah Hammond. *Fintech, Regtech and the Role of Compliance: A Regulatory Opportunity or Challenge?* Thomson Reuters, 2016.

Financial Conduct Authority. "Call for Input: Supporting the Development and Adoption of RegTech ." 2015.

Financial Conduct Authority. "Feedback Statement: Call for Input on Supporting the Development and Adopters of RegTech." 2016.

Financial Stability Board. "Financial Stability Implications from FinTech." 2017.

Goodspeed, Ingrid. "Cost of regulatory compliance in the aftermath of the global financial crisis." *SA Financial Markets Journal.* 2015. https://financialmarketsjournal.co.za/cost-of-regulatory-compliance-in-the-aftermath-of-the-global-financial-crisis/ (accessed 2018).

Gutierrez, Daniel. "Big Data for Finance - Security and Regulatory Compliance Considerations." *Inside Big Data.* 20 October 2014. https://insidebigdata.com/2014/10/20/big-data-finance-security-regulatory-compliance-considerations/ (accessed January 19, 2018).

He, Dong, et al. *Fintech and Financial Services: Initial Considerations.* IMF Staff Discussion Note, International Monetary Fund, 2017.

Hugé, François-Kim. "Using RegTech to Transform Compliance and Risk from Support Functions into Business Differentiators." *Inside Magazine - Edition 2018*, 2018.

Hugé, Francois-Kim, Carlo Duprel, and Giulia Pescatore. "The promise of RegTech. Elevating regulatory risk management in the financial industry to an effective business management practice." *Inside Magazine - European Union Edition*, 2017: 46 - 51.

Institute of International Finance. "RegTech in Financial Services: Technology Solutions for Compliance and Reporting." 2016.

Institute of International Finance. "RegTech: Exploring Solutions for Regulatory Challenges." 2015.

Internal Revenue Service. *Foreign Account Tax Compliance Act.* 16 March 2018. https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca (accessed June 2018).

Ivanoski, John M., Mike Walters, Deborah Bailey, and Jyoti Vazirani. "The transformative power of regtech." *KPMG.* 2017. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/06/transformative-power-of-regtech.pdf (accessed 2018).

Kamesam, Vepa. "Recent Technological Developments in Indian Banking." *Money, Banking & Finance Vol. 46*, 2003.

KPMG International. "2016 Global CEO Outlook." 2016.

KPMG. "The nexus between regulation and technology innovation." 2017.

Liebergen, Bart van, and Matt Ekberg. *Improving global AML efforts with technology and regulatory reform.* Briefing, Institute of International Finance, 2017.

Marlin, Steve. *Top 10 op risks: IT disruption heads 2018 poll.* 2018. https://www.risk.net/risk-management/5426111/top-10-op-risks-it-disruption-tops-2018-poll (accessed June 2018).

Mills, David , et al. *Distributed ledger technology in payments, clearing, and settlement.* Finance and Economics Discussion Series, Federal Reserve Board, 2016.

Petrasic, Kevin, Benjamin Saul, and Helen Lee. *Regtech rising: automating regulation for financial institutions .* White & Case, 2016.

PricewaterhouseCoopers. *IFRS 9 for banks - illustrative disclosures.* PricewaterhouseCoopers, 2017.

TABB Group. "Financial Markets: Embracing RegTech." 2017.

Toronto Centre. "FinTech, RegTech and SupTech: What They Mean for Financial Supervision." Note, 2017.

Transatlantic Policy Working Group Fintech. *The Future of RegTech for Regulators: Adopting a Holistic Approach to a Digital Era.* Innovate Finance, 2017.