Financial innovation

RegTech and SupTech – change for markets and authorities

Contact: patrick.armstrong@esma.europa.eu[52]

Regulatory and supervisory technologies are developing in response to various demand and supply drivers. On the demand side, regulatory pressure and budget limitations are pushing the market towards an increased use of automated software to replace human decision-making activities. This trend is reinforced by supply drivers such as increasing computing capacity and improved data architecture. Market participants are increasingly using new automated tools in areas such as fraud detection, regulatory reporting and risk management, while potential applications of new tools for regulators include greater surveillance capacity and improved data collection and management. With these new tools come challenges and risks, notably operational risk. However, with appropriate implementation and safeguards, RegTech and SupTech may help improve a financial institution's ability to meet regulatory demands in a cost-efficient manner and help regulators to analyse increasingly large and complex datasets.

Background

A combination of supply-based developments and demand-based needs are potentially transforming the way financial institutions comply with regulation and supervisory authorities oversee market participants. This article first seeks to identify the driving forces of this change, and why it is happening now. The article goes on to identify some of the key uses of the technologies being developed and the challenges and risks these technologies may introduce. The analysis has benefitted from numerous correspondence with technological firms at the coal face of these advances, as well as from contact with other global regulators that are seeking to understand how new tools can be best deployed.

The use of technology for compliance and supervisory monitoring predates the financial crisis of 2007. However, the new regulatory landscape, developed in response to the crisis, has been a catalyst for greater use of technology. The use of new technology in this context is evolving on a continuous basis and may soon lead to radical changes in the areas of compliance and supervision.

Foremost among the technological advances are the widespread use of **cloud computing**, the increased acceptance of **Application Programming Interfaces** (APIs) and advances in the fields of **AI and Machine Learning** (AI/ML).

Cloud computing allows for the use of an online network of hosting processors, increasing the scale and flexibility of computing capacity. APIs comprise rules and an interface for communication and interaction between different software programmes. AI is the theory and development of computer systems able to perform tasks that traditionally require human intelligence. ML, a form of AI, is a method of designing a sequence of actions to solve a problem that automatically optimises through experience and with limited or no human intervention.

RegTech describes technology, particularly information technology, used in the context of regulatory compliance, including tasks such as risk management. SupTech is technology used by supervisory authorities.

The next section of this article outlines factors underlying the growth of RegTech and SupTech, characterised in terms of demand and supply, and outlines how these drivers can interact in what is known as a 'regulatory dialectic'. The article goes on to present and discuss RegTech applications by market participants and SupTech applications by firms and describes some challenges for market participants and regulators.

[52] This article was authored by Patrick Armstrong and Alexander Harris.

Drivers

RegTech and SupTech are developing in response to various demand and supply drivers. Demand factors are linked to regulatory changes and market participants' and supervisors' need to process large amounts of data. Supply factors are primarily advances in technology.

Demand drivers

— The regulatory requirements placed on market participants have increased greatly over the past ten years. While many of these regulations were introduced in response to the known market failures that led to and exacerbated the global financial crisis, others reflect the increasingly complex nature of global financial services. Failure to comply with the regulations has significant consequences, which has in turn led to large spending increases on compliance and risk management programs by firms. Examples include increased reporting and compliance obligations implemented pursuant to the Dodd-Frank Act in the US and within the EU the Markets in Financial Instruments Directive (MiFID II).

— There is a continual push for efficiencies and cost savings, particularly for back-end and legacy systems as well as for labour-intensive processes.

— As the financial services sector becomes increasingly digitalised and data-driven the advantages of technology-driven compliance monitoring compared with less automated alternatives have become more and more evident. The increased volume of information needed to monitor and evaluate regulatory compliance creates challenges for enterprise data governance, but also opportunities to use the information for better risk management. Examples include developments in stress testing and enhanced risk monitoring.

— Government-driven mandates in some countries have led firms to implement technologies such as APIs and more effective authentication methods. An example is the Revised Payment Services Directive ('PSD2') in the EU.

— ESMA believes the move towards a more data-driven and pro-active approach will enhance monitoring of the financial sector and help ensure better outcomes for market participants and consumers. As we move towards this more intense, data-driven supervisory process, supervisors and regulators need to adapt. Failure to do so risks undermining the many years of work involved in implementing regulations.

Supply drivers

— In recent years, there has been a sharp drop in the costs of computing power and storage. This enormous increase in capacity is acting as an important catalyst for AI/ML tools, which are extremely data-intensive. Many of these tools are at the heart of the RegTech/SupTech renaissance and could not be deployed in a non-digital infrastructure. For example, cloud computing provides remote access to servers on which large amounts of data can be stored.

— Improved digitalised data architecture minimizes interoperability, reduces redundancy and allows for improved communication among data centres.

— Advances in AI and big data offer new capabilities. For example, pattern-recognition using ML algorithms has wide applications, including in monitoring markets for potential misconduct.

Regulatory dialectic

The emergence of RegTech seems a predictable response to the post-crisis regulatory agenda. It is a clear example of the "regulatory dialectic", whereby regulatory action on the part of public authorities is met by a private-sector response designed to ameliorate the impact of regulations. In some cases, this response may aim to side-step regulations, which may prompt the authorities to tighten the regime further. In other cases, market participants respond by managing their regulatory requirements more efficiently. RegTech fits in to the latter scenario, as it is designed to help firms adapt to regulation in an effective, cost-efficient manner.

RegTech applications by market participants

Regulatory pressure and budget limitations are pushing the market towards an increased use of automated software to replace human decision-making activities. AI/ML tools are often used to implement such automation, with the calibration of the tools based on the recognition of patterns and relationships in large amounts of structured or unstructured data (big data). This section examines the most relevant technologies used in such contexts.

AI and ML

AI/ML techniques can be used to find patterns in large amounts of data from increasingly diverse and innovative sources. AI is a broad field, of which ML is considered a sub-category. Financial firms are exploiting such technologies in the following contexts: (i) customer-focused (or 'front-office') uses such as credit scoring, insurance, and client-facing chatbots; (ii) operations-focused

(or 'back-office') uses, including capital optimisation, model risk management and market impact analysis; (iii) trading and portfolio management in financial markets.

Big data

'Big data' is a term used broadly to describe the storage and analysis of large and/or complicated data sets using a variety of data elaboration techniques. AI/ML tools are generally used in a big data environment, allowing the implementation of new data management platforms that can capture, store and analyse enormous volumes of structured and unstructured data. Financial firms can feed the new data platforms with a variety of data sources:

- Internal sources: customer data are a primary form of proprietary internal data, along with data on all internal operations (assets, liquidity, loans, payments, etc.). Whether from internal or external sources, personal data are subject to strong privacy safeguards under EU legislation. Many datasets are unstructured, making them difficult to work with using traditional infrastructure.
- External sources: a myriad of third-party specialized data providers offer data related to specific contexts, typically via open real-time software interfaces and with standardised query methods.

This large amount and variety of data can be exploited by financial firms using big data technologies to improve business, assure regulatory compliance and analyse trends. Some common RegTech applications by banks and financial services firms are:

- Fraud detection: banks and financial firms use analytics to recognise fraudulent transactions.
- Reporting: regulations require financial firms to report specific business data to authorities.
- Risk management: regulatory schemes require firms to manage a variety of risks in a proper way (e.g.: liquidity risk, operational risk).

SupTech applications by regulators

Regulators are increasingly harnessing the benefits of technology. For example, compliance reporting has frequently not been as efficient as desired. Financial institutions often need to submit information in response to ad hoc requests from regulators. The non-machine-readable data submitted by financial institutions makes the application of data analytics by regulators difficult and time consuming. In turn, some regulators have been investigating how FinTech can be used to make supervision more effective, to improve surveillance and to reduce the compliance requirements imposed on financial institutions.

Potential applications of AI/ML

An area of interest for regulators is the application of AI/ML. Authorities such as the ECB and the US Federal Reserve are using natural language processing (NLP), a form of AI, to help them identify financial stability risks.

Another potential application of AI/ML is to detect trade syndicates in the securities market. Collusive behaviour and price manipulation can be especially hard to detect using traditional methods. Rule-based systems, such as transaction-monitoring systems, have very high false-positive rates, bringing extra, costly, work to both exchanges and regulators. Another challenge that AI/ML tools could help to tackle is complicated network analysis, especially when the network is large and changes over time.

Finally, a challenge for the application of AI/ML arises when a potential misconduct case is detected. At present, external human experts are required to verify that such cases warrant further investigation. As experts are costly to employ and very limited in number, regulators would benefit from any potential extension of AI/ML technologies to this context.

Recent attempts to use ML to detect potential cases of market abuse show some promise. Some regulators, such as the UK Financial Conduct Authority (FCA), have been exploring how best to analyse large datasets to study suspicious trading behaviour. In this context, AI/ML tools may help to identify cases of collusion to manipulate share prices or circular trading to create a false impression of market interest.[53] Such tools can be tested with market data to generate better detection outcome as a result of the following aspects:

- Compared with the high false-positive detection rate of traditional rule-based surveillance systems, ML based surveillance systems have, through mathematical optimisation techniques, been able to reduce false positive rates.
- Some regulators are employing technological tools to reduce the need for humans to manually conduct complicated network analysis. This approach involves analysing years of raw order book data with modern network-analysis techniques. The benefit of this system is not only the processing of large

[53] Relatedly, regulators such as the Bank of Italy are developing AI/ML tools for AML detection.

volumes of data, but also the detection of complicated network relationships across long time periods and often involving substantial numbers of participants.

— ML approaches, especially semi-supervised ML algorithms, can handle certain cases for which human experts' judgement has traditionally been required. In particular, NLP[54] technology could be used to automatically analyse the historical case document and extract meaningful information on which ML algorithms can operate.

Preliminary work by authorities using big data processing systems has made clear that many years of transaction data and even order book data can be analysed. However, further improvement and refinement of these ML-based systems is needed, due to the limited availability of training cases. Other challenges include how ML can be used to detect unknown misconduct and how the results from the ML algorithms can be interpreted.

Risks and challenges for regulators and market participants

Improving data collection and management

A critical step in transforming financial supervision is improving data collection. Currently, the prevalent approach to data collection by regulatory authorities is periodically collecting data in the form of standard reporting templates. Much of the current focus is on creating reporting templates, rather than on the primary data constructing the desired reports. Regulatory reporting can be challenging for financial institutions and is often resource-intensive.

Increasingly, regulatory authorities are exploring opportunities to automate the regulatory processes and create reporting utilities. These are centralised structures that act not only as a common database of reported granular data but also as a repository of the interpretation of reporting rules in a format that is readable by computers. RegTech is therefore offering an alternative and a move away from templates and manual procedures. In the move towards a data-driven supervisory or compliance process, the cleanliness and accessibility of the underlying data is paramount. The use and accuracy of tools such as AI/ML relies upon the strength of the underlying data. This means that prior to the use of data, regulators and supervisors must have the appropriate procedures and systems in place to ensure that the data they receive are of good quality. One possible solution to achieve this is to develop machine-readable regulations, in particular in the field of regulatory reporting. Indeed, the use of IT solutions can help regulators to standardise and codify the information they receive from market participants, making it easier to manage and use the data.

Digital transition

In the wake of the financial crisis, much of the global regulation implemented is highly dependent on technology. A failure on the part of market participants to adapt to the new digitalised infrastructure represents a business risk that may separate winners from losers in the coming years. In addition, failure to adapt to a more automated regulatory compliance process may leave participants with platforms that are ill-suited for the current regulatory framework.

For their part, many in the regulatory community are moving increasingly towards a data driven supervisory process. To process such data, regulators need to invest in the technological tools and human skills that will allow them to effectively analyse the results.[55] In turn, regulators must migrate to a digital-based supervisory process; only then will they be able to cope with the volume of data they will soon receive.

Operational risks

As both regulators and market participants move towards a digitalised architecture, risks related to cyber resiliency must become a core part of their supervisory and compliance strategies respectively. Indeed, as market participants and regulators become increasingly interconnected through regulatory reporting, security risks increase. In addition, reliance on APIs, cloud computing and other new technologies that create increased interconnectivity could potentially make the system more vulnerable to cyber-threats and expose large volumes of sensitive data to potential breaches. A related form of operational risk arising from a move towards greater use of data and risk management tools via third-party providers is concentration risk.

Regulators and market participants will therefore need to devise and implement appropriate strategies to manage these operational risks. To this end, it is important that market participants and regulators cooperate to promote effective

[54] NLP is an interdisciplinary field of computer science, AI and computation linguistics that focuses on programming computers and algorithms to parse, process and understand human language.

[55] One approach may be to set up specific initiatives, such as the Data Science Hub recently set up by the Netherlands Bank. For more detail see Broeders and Prenio (2018).

management and control of cyber-risks and to enhance cyber-resilience.

Risks from strategic incentives

One risk that authorities should bear in mind when developing automated detection tools is the possibility that malicious agents may learn to frustrate the tools by adapting their behaviour. For instance, market participants could, in theory, learn what types of behaviours are likely to cause a flag in a SupTech monitoring system. Using such information, firms might be able to structure their regulatory returns in such a way as to remain undetected. Separately, as firms develop their expertise in RegTech, their systems may become able to identify potential regulatory loopholes.

Conclusion

Just as FinTech is introducing changes to the way in which market participants offer their services, so too will RegTech and SupTech alter the way in which financial institutions and regulators, respectively, comply with the rules and supervise markets. In so doing, these technologies have the potential to reshape the relationship between regulators and market participants. For example, technologies such as APIs are facilitating more efficient filing of regulatory data by market participants, while regulators are looking to develop AI/ML tools to enhance their market surveillance and to improve their capacity for fraud detection. Inevitably, new technological abilities bring with them new challenges and new sources of risk, notably including operational risk. Nonetheless, provided they are implemented correctly and monitored effectively, RegTech tools have the potential to improve a financial institution's ability to meet regulatory demands in a cost-efficient manner and help regulators to analyse increasingly large and complex datasets.

References

Broeders, D. and Prenio, J. (2018), "Innovative technology in financial supervision (suptech) – the experience of early users", FSI Insights No. 9.