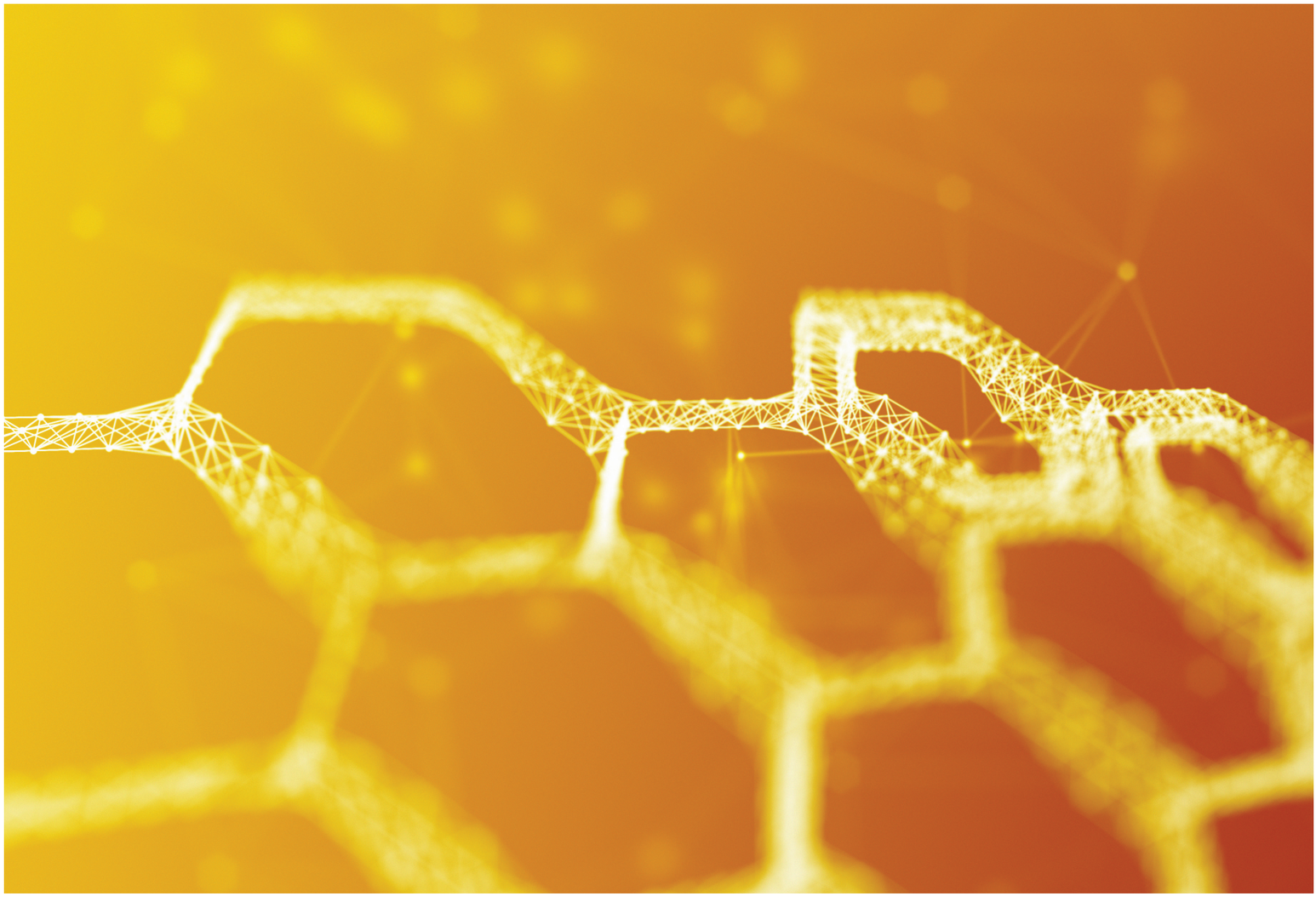
Risk publications

Regtech

Risk.net May 2017

Special report



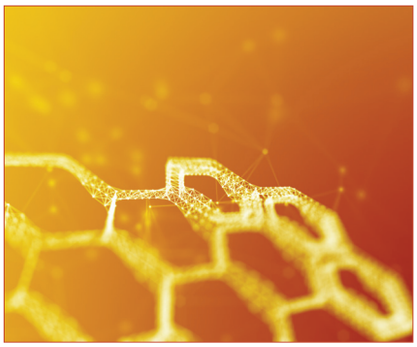
Risk.net

Sponsored by

Wolters Kluwer

ORACLE®

FINANCIAL SERVICES



Wei-Shen Wong, **Asia Staff Reporter**
wei-shen.wong@incisivemedia.com

Harjeet Singh, **Publisher**
harjeet.singh@incisivemedia.com

Stuart Willes, **Commercial Editorial Manager**
stuart.willes@incisivemedia.com

Marcel Chambers, **Commercial Director**
marcel.chambers@incisivemedia.com

Celine Infeld, **Managing Director**
celine.infeld@incisivemedia.com

Lee Hartt, **Group Publishing Director**
lee.hartt@incisivemedia.com

Ryan Griffiths, **Senior Production Executive**
ryan.griffiths@incisivemedia.com

Incisive Media (UK)
Haymarket House, 28–29 Haymarket
London SW1Y 4RX
Tel: +44 (0)20 7316 9000,

Incisive Media (US)
55 Broad Street, 22nd Floor
New York, NY 10004-2501
Tel: +1 646 736 1888

Incisive Media (Asia-Pacific)
Unit 1704-05, Berkshire House
Taikoo Place, 25 Westlands Road,
Hong Kong, SAR China
Tel: +852 3411 4888

Twitter @riskdotnet
Facebook facebook.com/riskdotnet
LinkedIn Risk.net

Cover image
Shulz/Getty

Published by Incisive Risk Information Ltd

The dawn of regtech

We live in an age where there is no shortage of new regulations. Not only do firms need to think about being compliant in the jurisdiction in which they are headquartered, they must also monitor the evolving regulatory landscape in the various markets that they want to participate in. Whether North America, Europe or Asia, the tentacles of Mifid II, IFRS 9, FRTB, Emir, General Data Protection Regulation (GDPR) and Dodd-Frank are far-reaching.

Banks constantly need to inject funds into their compliance budgets – for internal staffing needs as well as to improve systems and processes. Enter regulatory technology, or 'regtech' as it has become more popularly known. Put simply, regtech is a classification of technology specifically addressing regulation and compliance issues in the financial industry.

This special report looks at how the regtech industry is being driven by firms' unpreparedness towards new reporting needs and how they are scrambling to find solutions to implement within the tight time frames. However, while this environment presents opportunities for solution providers, it is beginning to weigh heavily on the shoulders of end-user firms (see page 12).

We break down the relationship between regtech and the wholesale banking industry. Although technologies such as voice recognition and cloud computing – among others – are gaining traction, they seem to be less of an immediate game-changer within wholesale banks. While investment banks are aware of the shift in the technology world, a meaningful use is yet to be found for these technologies in their operations. Our fintech feature discusses the reasons for this lag and what realistic changes the industry can expect (see page 15).

One of the most talked-about technologies on the conference scene is blockchain. We look back at the evolution of how blockchain and distributed-ledger technologies became buzzwords, and touch on the digital currency, bitcoin (see page 24).

We explore what Brexit means for the UK and the practicality of Mifid II implementations once the UK is formally separated from the European Union. Due to the large volumes traded in the UK, it is unpredictable to know – for example – how leaving UK data out of the equation will impact such things as Mifid II calculations and assessments (see page 18).

One of the reasons firms are trying to either seriously beef up their compliance systems or find a third-party solution is to avoid being slapped with hefty fines, such as for the GDPR, which will come into effect in May 2018. If banks suffer a serious data breach, they can face fines of up to 4% of their global turnover. Potential cyber attacks that result in serious data breaches are encouraging banks to review and overhaul their internal systems and processes (see page 7).

We look at how machine-learning techniques can help risk managers do their job more efficiently and improve risk modelling. Some dealers have explored applying artificial intelligence to operational risk and anti-money laundering modelling (see page 4).

Circling back to blockchain and its potential as a real-time market surveillance tool, our feature on page 23 looks at a group of banks and tech firms that tested using blockchain and smart contracts for the affirmation and post-trade lifecycle management of equity swaps.

There is no shortage of so-called regtech solutions available in the market, but it still comes down to how firms choose to handle their compliance issues, and whether or not those methods enable firms to focus on their core business while at the same time remaining compliant.

Wei-Shen Wong,
Asia staff reporter

Leading the way

Risk has been at the cutting edge of risk management, derivatives and complex finance since 1987.

But we're not dwelling on the past. By looking continually forward and covering these markets in unparalleled depth, we keep our readers ahead of the game.

Thanks for your support. Here's to the next 30 years.

Risk.net

Automatic for the people

Banks are straining to comply with regulator-drafted guidelines introduced to prevent them suffering losses from decisions based on poorly crafted models. This burden is pushing some firms to explore opportunities afforded by machine-learning technologies – though many have reservations. By Louie Woodall

Need to know

- Regulatory initiatives in the US, European Union and UK have turned the spotlight on to banks' model risk management processes.
- The resulting increased workload on model risk managers is sparking interest in automated processes to help alleviate the burden of certain tasks, such as data cleansing and model validation.
- "If machine learning can help develop a heat map to show where managers should be placing their attention and what models need to be refined, that would help focus their efforts," says Ed Young at Moody's Analytics.
- However, consultants and dealers say supervisors are suspicious of the use of 'black box' algorithms whose workings banks cannot clearly explain.
- Banks may also struggle to graft machine-learning technologies on to legacy systems.

It's tough being a model risk manager these days. In the US, global investment banks and domestic lenders alike continue to grapple with prudential guidance on model risk management, known as SR 11-7. Meanwhile, their European counterparts recently began welcoming onsite inspectors under the European Central Bank's (ECB's) Targeted Review of Internal Models (Trim) programme.

UK model teams also have their work cut out. At the end of March, the Bank of England issued a letter to British banks and building societies outlining the model management principles they expect their charges to adhere to.

These regulatory initiatives (see box: *New model army*) aim to nix the threats posed by unruly models by regimenting the model validation process within banks. But many claim expectations of the model risk management function are outpacing banks' ability to adapt – with potentially dire consequences.

Floundering amid the wave of new duties assigned to them, model risk managers are understandably seeking a life preserver – and some think they've spotted one. Dealers are increasingly exploring the possibilities offered by machine-learning algorithms that can make sense of large, unstructured datasets and police the outputs of primary models.

"I am a big supporter of the use of machine learning and computational intelligence in model risk management, not only for the development of model benchmarks but also to facilitate the validation process itself," says Lourenco Miranda, head of model risk management for Americas at Societe Generale in New York. "Humans would never be replaced for the more complex decisions in model risk, but by training a machine to process repetitive parts of validation we can focus our attention on the higher and more complex models responsible for the biggest exposures. It is a great increase in efficacy of the model risk management process."

Others are less taken by the promise of

machine learning, however: "The short answer is we are not there yet," says the head of model risk at an international bank. "I think it's definitely an area to be looked into in the future. But from a practical point of view, the risk management platforms of the banks are very heavy. It's very difficult to change them."

He's not alone in his reservations: academics have also warned that machine learning should not be seen as a silver bullet. Yet so long as the regulatory focus on model risk shows no signs of abating, it seems likely managers will continue to seek new technologies to make their lives easier.

"Anything that could improve the data-processing and data-cleaning processes would be good, because to tell the truth a good deal of our validation work is on data issues. What I had in mind was to look at whether these solutions can be used in our model environment to replace and automate data treatment and to replace human intervention," says the head of model validation at a regional European bank.

Reducing the spadework

With resource-strapped model validation teams overloaded and their in-trays filling up, many are enthused by the potential for machine learning to smooth those parts of the process that are most labour intensive and prone to error.

"The amount of work to do on an ongoing basis to demonstrate to regulators that models are operating properly is overwhelming and very manually intensive. If machine learning can help develop a heat map to show where managers should be placing their attention and what models need to be refined, that would help focus their efforts," says Ed Young, senior director in capital planning and stress testing at Moody's Analytics in New York.

Machine-learning algorithms allow computer programs to make decisions and predictions from unseen data inputs. Two principal subsets exist: 'supervised learning' algorithms, which are taught through example datasets to map certain inputs to outputs, and 'unsupervised learning' algorithms, which are presented with datasets and left to discover patterns on their own, without human guidance.

French dealer Natixis is one firm getting to grips with the possibilities of unsupervised learning algorithms in model validation. For the past six months, its equity derivatives business has utilised this type of machine learning to detect anomalous projections generated by its stress-testing models. Every night, these models produce over 3 million computations to inform regulatory, internal capital allocations and limit monitoring. A small fraction of these are incorrect, knocked out of the normal distribution of results by a quirk of the computation cycle or faulty data inputs.

"This machine-learning algorithm helps us to determine which results are suspicious, so that we can analyse them and automatically replay the computation in case it was caused by a transient error. All results are scanned and evaluated by the machine learning regardless of the final use of the projections, whether for regulatory or trading purposes," says José Luu, head of IT derivatives and pricing at Natixis in Paris.

This use of machine learning hands validators a valuable tool for the ongoing monitoring of their stress-testing models, as it can help determine whether they are performing within acceptable tolerances or drifting from their original purpose.

Nomura is another dealer that has been using a form of machine learning as part of its model risk management function, specifically to police model use – something it has been doing for the past six years.

Slava Obraztsov, global head of model validation at Nomura in London, says: "We record model restrictions in a machine-readable format to support their automated monitoring. What happens is we validate a model and impose restrictions on what products it can be used for. The monitoring is run across all trading portfolios on a periodic basis to check that no position has been booked on a model in breach of its restrictions. This is to ensure that products are not booked on models that may not properly capture some product features and dynamics."

Other dealers have been exploring and implementing machine learning in relation to operational risk and anti-money laundering (Amachine learning) modelling, says Shaheen Dil, New York-based managing director at consultancy Protiviti.

"The reason is that these are the two areas of risk where the datasets are enormous. In the case of operational risk there are no standard acceptable models that have been in place for a long time, so banks have had to build their own from scratch. For Amachine learning, many banks are purchasing vendor models, but these are by and large 'black boxes' to the banks," says Dil.

Valid arguments

Validation appears to be the area with the most to gain from embracing machine learning, as it comprises a number of tasks that could benefit from automation. SR 11-7 pushes banks to conduct periodic reviews "at least annually" of all models to ensure they are working as intended, covering everything from their "conceptual soundness" – essentially their design and construction – to their sensitivity to small changes in data inputs.

Ongoing monitoring is also expected: internal and external data should be checked and re-checked, computer code subjected to "rigorous quality and change control procedures", reports generated from model outputs reviewed, and the models themselves benchmarked to estimates from internal "challenger models" or third-party calculation engines. All this must also be documented in sufficient detail such that an independent third party – an auditor, for instance – could make sense of it.

The Trim also advocates an annual validation cycle at a similar level of granularity. Right now, this is beyond the capabilities of some banks.

"We do not comply completely; we do not review all the models every year," says the head of model validation at the regional European bank.

"We don't have the means. I am not afraid about the utility of our models, but the ECB expects us to have a formal, standardised process and right now our function is decentralised and not globally co-ordinated."

Data quality is a particular focus of the Trim. For example, in the context of the internal ratings-based approach for credit risk capital, the ECB expects input data for these models to be subject to periodic cleansing analyses, as well as benchmarked against external up-to-date credit data sources.

Dealers say machine-learning algorithms can monitor and identify patterns in data faster and more efficiently than hard-coded programs and identify missing inputs that, if located, could upgrade a model's performance.

"If you go to the banking book, we have a lot of products that have different patterns, different structures. We currently use econometric models for the prediction of the data. Machine-learning classification can be used and then the production of the model can be done correctly. The projection of the risk by machine-learning techniques is also much more accurate and robust," says Mostafa Mostafavi, London-based vice-president of risk and quantitative analysis at Credit Suisse.

Take the example of validating an op risk model that measures losses from fraud. A machine-learning algorithm could examine all the inputs that go into predicting fraud losses and identify missing pieces of information that, if added to the statistical model, could improve its performance, suggests Dallas-based Chris Siddons, senior director of regulatory and compliance software at LexisNexis Risk Solutions.

Machine learning could also be harnessed for model benchmarking purposes. "Many larger banks need to build challenger models to test the primary models for accuracy and robustness. Machine-learning algorithms can function as challenger models or for checking specific aspects of the primary models' predictive power," says Marco Vettori, a partner at McKinsey in Milan.

The consultancy is also tipping machine learning to advance into the building of primary models themselves – something at least one dealer is already getting to grips with: "We use machine learning to build primary models, including our CCAR [Comprehensive Capital Analysis and Review] models," says the head of risk analytics at a second international bank. "Machine learning is used to cluster and segment data to construct each model as well as for model calibration. This year these technologies have been much more heavily used in-house."

Fear of the unknown

Yet plenty stands in the way of a full-scale march of the machines. First, certain banks are nervy about the attitude regulators will take towards these complex technologies. Second, banks themselves may be struggling to understand the biases implicit in these machine-learning models and substantiate them to their own satisfaction.

As these are learning algorithms, it's hard for a model risk manager to prove how a machine-learning technology reaches its conclusions. If something's hard to prove, it's hard to document – something essential to the model risk management process.

"Regulators require banks to explain why a decision was made and machine learning doesn't allow for that. There are some efforts to tag machine-learning outputs with explanations, but it's not a natural part of the process," says Ranko Mosic, a Toronto-based big data consultant who has worked with Bank of America and State Street, among others.

Yet Credit Suisse's Mostafavi believes regulators aren't as scared of machine learning as these consultants suggest. "Because they are not simple, people think they are not transparent, but I think they are good tools. This is a growing area; machine-learning software will be used frequently in the future," he says.

Grafting machine-learning technologies on to legacy systems is no walk in the park for the dealers themselves – another reason wholesale adoption does not yet appear to be on the cards.

"A problem in large corporations is the sheer complexity of machine learning. Firms have enough trouble with their existing processes – extract, transform, load, solving data silo problems and modelling. With machine learning it's not as simple as rolling out a new packaged or in-house built data system. Some firms don't know where to start," says Mosic.

Nonetheless, investing in better model risk management is worth the expense when considering the alternatives, many point out. ■

Previously published on Risk.net

NEW MODEL ARMY

The challenges facing banks' model risk managers are stiff. The Federal Reserve's SR 11-7 has become the gold standard for model risk management since its unveiling in 2011; but, despite being in effect for six years, few banks are adhering to it to the letter. Dealers have previously reported that the guidance impelled a threefold increase in the number of models requiring validation and a vast expansion of staff assigned to the model risk function.

Dealers say foreign regulators have effectively cribbed the Fed's guidelines for their own supervisory standards, extending SR 11-7's reach far beyond US shores. For instance, the principles set out in the Bank of England's letter to British banks and building societies on model governance represent "a concise and mature representation of the SR 11-7 text", according to the head of model risk at one international bank.

The themes addressed by the European Central Bank's Targeted Review of Internal Models (Trim) programme are also "very similar" to SR 11-7, says Konstantina Armata, head of global model validation and governance at Deutsche Bank in London.

"These are big exercises; we are talking about weeks and weeks of examinations and hundreds of requests. It's a big process for us," she says.

SR 11-7 sets out compliance requirements across four broad categories of model risk management: development and implementation, use, validation and governance. To manage these simultaneously, most banks have consolidated their model risk management functions under one roof.

This organisational overhaul was only the first step on the journey to compliance, however. Dealers may have made progress building model inventories, assigning model owners and setting up independent validation processes, but there is still much work to be done getting the models themselves up to scratch – and verifying their effectiveness.

"In the case of the biggest challenges for SR 11-7, I would say that model preparedness is number one. Despite the guidance being now six years old, there is still a lot to be done in terms of preparedness: model documentation, internal control testing and documentation of the results, continued monitoring of the impact of model limitations, and so forth," says Lourenco Miranda, head of model risk management for Americas at Societe Generale.

The great data protection race

The cost of implementing the EU's forthcoming General Data Protection Regulation could cost the largest banks hundreds of millions. But with cyber attacks on the rise, many are quickly dipping into their pockets. By Alina Haritonova

Need to know

- The EU's General Data Protection Regulation (GDPR) will upend the way banks process and disseminate customer data.
- Banks will need explicit consent to retain customer data, forcing them to undergo vast data mapping exercises and review all relationships with external suppliers.
- Firms that fail to comply, or suffer serious data breaches through cyber attack, for instance, face fines of up to 4% of global turnover.
- GDPR enshrines in law the "right to be forgotten" – the right of individuals to obtain personal data relating to them from a firm and, provided certain conditions are met, request its deletion.
- Compliance costs for the largest banks could run to hundreds of millions of euros.

Banks are no strangers to the perils of lax data security. The growing frequency and severity of cyber attacks on lenders have made resilience against external attack a top operational risk priority for banks. To ensure practitioners' minds are sufficiently focused, however, European supervisors are introducing tough new legislation on data protection standards – seemingly favouring the stick over the carrot.

Under the EU's forthcoming General Data Protection Regulation (GDPR), due to take effect in May 2018, banks can face mind-boggling fines of up to 4% of their global turnover if they suffer a serious data breach. To put that in context, had the GDPR been in place at the time of the cyber attack that hit Tesco Bank in early November 2016 – which resulted in the theft of some £2.5 million ($3.1 million) from customers' accounts – the bank would have been handed a £1.9 billion fine according to some estimates, not to mention a raft of potential new avenues for customers to pursue legal settlements.

A Tesco Bank spokesperson says: "There is no evidence to believe there was a compromise of personal identity information."

Understandably, the headline numbers have grabbed the attention of dealers. The proliferation of cyber attacks resulting in serious data breaches – and the penalty they could face for such breaches in future – has pushed banks to undertake a serious overhaul of internal systems and processes, as well as a wholesale review of relationships with external vendors that process customer data on their behalf.

"The fear of significant fines is driving [banks] to spend a lot of money working out how to get compliant. The relevant outsourcers also have a lot of work to do," says a senior consultant at one professional services firm in London. "Regulators see GDPR as an evolution of existing privacy laws. But unfortunately, I would say 80% of organisations do not comply with existing privacy legislation."

The introduction of the GDPR marks a significant shift from the existing EU data protection regime, superseding the patchwork of national legislative

£1.9 billion

The fine Tesco Bank could have faced under the GDPR after the November 2016 cyber attack

regimes loosely bound by the existing EU Data Protection Directive, promulgated in 1995.

Crucially, GDPR is explicitly extra-territorial in scope: its new, more stringent standards will apply to overseas firms that process the personal data of EU citizens if the processing activities are linked to the "offering of goods and services" or "the monitoring of their [EU-based data subjects'] behaviour".

In practice, this means US and Asian dealers that service European clients, for instance – as well as the subsidiaries of European banks in other countries – will have to comply with the regulation.

"Any organisation that collects private information on individuals in the EU – no matter where that organisation is domiciled – will be impacted," says Stephanie Snyder, national sales leader for Aon's professional risk solutions practice in Chicago.

Keeping records of processing activities and compliance practices – and being able to demonstrate whether client consent to retain data has been sought – are among the key requirements for banks that find themselves in scope.

This will necessitate undertaking vast data mapping exercises, say banks, as well as increasing monitoring of firms that process data on their behalf. In the case of the largest banks, that means reassessing – and where necessary, re-papering – legal agreements with thousands of external suppliers, adding clauses to agreements such as the requirement to obtain prior written consent from controllers if they wish to sub-contract work out.

GDPR builds on the taxonomy set out in the original EU directive. Bank customers will still be categorised as 'data subjects', as they are under most existing national governance regimes, but will gain new rights around the ability to access data banks hold on them, and the right to request its removal.

Banks or other financial firms that process large amounts of client data will be regulated as data controllers – as they currently are – but will face beefed-up requirements, such as the need to appoint a dedicated data protection officer (DPO) where they engage in "regular and systematic monitoring of data subjects on a large scale".

But the regime also assigns many of the same legal responsibilities that apply to data controllers around data security, transfer and record-keeping to data processors, too – external vendors that process data on controllers' behalf. In the case of firms that act as processors in the financial markets, the requirements could affect everyone from database managers to market research firms.

Observers suggest the change reflects the growing number of critical functions outsourced to external vendors by many firms that hold large amounts of data – and is long overdue.

"The reality is the lines between who is really controlling the personal data – who is the processor and who is the controller – are increasingly blurred. One of the things the GDPR does is change the rules substantially for those people who once called themselves just processors," says Richard Jeens, a London-based partner at law firm Slaughter and May.

> "Any organisation that collects private information on individuals in the EU – no matter where that organisation is domiciled – will be impacted" Stephanie Snyder, Aon

Andrew Stacy, UK-based business development director at tech vendor Glassbox, suggests the regulation is likely to see firms previously defined as data processors being pushed into the data controller category.

"You might have a broker that sells the products of multiple companies. In that capacity, they would be operating as a data processor – but they'll have details of their customers, so they will also be registered and regulated as a data controller in their own right," he says.

Crucially, GDPR also empowers national supervisors to enforce breaches of the rules against non-compliant firms. Supervisory bodies – for instance, the Information Commissioner's Office in the UK – will have an array of tools at their disposal to investigate and weed out non-compliance. These include on-site inspections, the right to issue public warnings on firms, and imposing corrective sanctions.

Top-down scrutiny will also increase. Under Article 29 of the old directive, a working party was set up to offer guidance to member states on uniform application of the rules, and to report back to the European Commission on the broad level of protection enjoyed by EU citizens. GDPR replaces the working party with a beefed-up European Data Protection Board, comprised of representatives of supervisory authorities appointed by every EU country, a European Data Protection Supervisor and a representative from the Commission.

Compliance concerns

Given the onerousness of the requirements, and the potential penalties for missteps, banks are understandably keen to make sure they are observing the rules to the letter. The trouble is, many say, too much is left unsaid in the level one text of the rules. Take, for instance, the requirement to appoint a DPO: according to the rules, data controllers and processors alike must appoint DPOs where their "core activities… require regular and systematic monitoring of data subjects on a large scale".

Lawyers point out, however, that the "large-scale" designation is not determined by a quantitative threshold, but rather is decided on a case-by-case basis. Given the fact that many vendors monitor large amounts of client data on behalf of banks, they are likely to fall within the scope – but many are unsure.

"Supposing you're a processor, you might be providing some processing services for personal data to a lot of clients… [which individually] might not be considered as large-scale," says Kuan Hon, a consultant lawyer at Pinsent Masons in London. "But if you add all the clients' sensitive personal data that you handle together, it might be considered large-scale – and then you as a processor for those clients will have to appoint a DPO."

Another area requiring banks' attention if they are to avoid hefty fines is how they go about notifying regulators and customers of data breaches. Currently, there is no overarching law governing notification of breaches at a European level – and in most member states there is no obligation whatsoever. For example, while the German Federal Data Protection Act includes an obligation that firms issue notifications when data breaches take place, this is purely voluntary.

In the Netherlands, the data breach notification regime does not include a fixed time period for notifying the regulator or allow controllers to investigate breaches – but non-compliant businesses can still face a fine of up €810,000, or 10% of the company's net annual turnover.

The time frame set for notifying regulators of breaches will become a lot clearer under the GDPR: firms must make contact with their regulator 72 hours after breaches become known. In addition, where a breach may have a significant impact on customers' rights and freedoms, controllers will

have to notify all the affected individuals, not just the regulator.

Others say this provision is subject to interpretation: "Actually, it's 72 hours after you've become aware of the personal data breach, and only where it's feasible. So the deadline is not set in stone," says Hon.

The GDPR also takes a stricter line on individuals' rights by enshrining in law the so-called "right to be forgotten" – the right of individuals to obtain personal data relating to them from a data controller and, provided certain conditions are met, request its erasure.

Again, some jurisdictions allow EU citizens to make similar demands already, but rights vary widely. Data subjects in the UK have the right to apply for a court order to rectify, block or destroy data – but this is only granted if the court rules the data is inaccurate.

Under Article 17 of the GDPR, the right to be forgotten applies when a data controller has no legal justification for keeping and processing personal information. For banks, that could prove highly problematic: most obviously, say practitioners, it could directly conflict with other obligations such as know your customer (KYC) rules, which require financial organisations to keep relevant records on customers in accordance with applicable laws.

Some are already warning the clause has the propensity to upend how banks deal with customer data.

"A bank may have legitimate reasons to hold back data, for KYC or legal reasons; but if there's no specific reason, they will have to work through all the records across the bank about you [with a view to deleting it]. And how do they delete it? It's difficult," says the senior consultant.

Banks are also concerned about the second-order effects of the clause. Enhanced rights will make it much easier for EU citizens to claim damages for compensation, say lawyers.

"There will be more focus on mitigating the increased risk of litigation – for instance, from lawyers targeting groups of individuals whose privacy has been infringed or data mishandled on a contingent or no-win no-fee basis," says Jeens at Slaughter and May.

Relatedly, GDPR also grants subjects the right to data portability; when customers consent to the processing of their data, or where processing is an essential part of a contract being fulfilled, they gain the right to access all relevant personal data an institution holds on them in a structured, commonly used and machine-readable format.

Where's the data?

Complying with this clause is likely to present a huge challenge for many banks: a 2016 report released by the Institute of Directors and Barclays highlighted that 43% of businesses, including banks, didn't know where their data was physically stored.

"You have a question around portability: an individual can say 'I want you to give me all the information [you hold] on me so that I can take that to another organisation'. If [banks] don't know exactly what information they hold, how do they pull that all together? Many organisations are supposed, under existing privacy law legislation, to only keep data for as long as it's necessary – but frankly, they keep it forever and don't necessarily delete records. Getting the process of deleting information in place is something many organisations aren't used to doing," says the senior consultant.

With scarcely a year before the regulation enters force, banks are working hard on implementation. The division of labour will vary from bank to bank, say practitioners, with the agenda set by the compliance division and the bulk of the implementation burden falling to operations and IT teams.

"Most of the implementation will be silo-orientated – but some of the solutions are horizontal and bank-wide, and for that we are wrapping up a central programme team. In some business lines, about 30 people can be devoted to implementing the change full-time," says the head of op risk at a European bank.

The overall number of internal staff required to meet this task at a big bank is in triple digits, some estimate, and sometimes even higher once external consultants – who may number 10–15% of the total – are taken into account. Consultants can step in to help banks document their processes, or else offer dealers strategic advice on how to achieve a passing grade.

Vast undertaking

One of the most onerous tasks banks have sought to outsource to consultants is a full audit of their external vendor networks in order to keep up with heightened compliance standards – a vast undertaking for the largest banks. A lot of supplier relationships will have to be re-assessed to ensure they are in line with the new rules, and in some instances commercial terms will have to be changed, say lawyers.

"When you appoint a new data processor – someone who can only process information on your behalf – you have to put certain provisions into that contract. Banks have supply chains with tens of thousands of suppliers. A couple of banks have talked about doing 18-month to two-year-long projects just to refresh all their supply chain contracts to include the new provisions. That's a huge amount of effort, so some of them have started engaging external consultants to do that. The cost of that is pretty huge," says Georgina Kon, partner at Linklaters in London. ■

Previously published on Risk.net

Wolters Kluwer

Meeting the daunting demand for data

Increasing regulation requires more data reporting, and financial institutions are relying on faster, more adaptable regtech solutions to manage the swelling scope and complexity of regulatory compliance and to build more efficient businesses. Rajat Somany, vice-president, product and platform management at Wolters Kluwer presents some solutions to meeting this demand in the face of current and impending regulatory barriers

Whatever opinion you may have about the job financial supervisors are doing, you could hardly call them insufficiently inquisitive. Lawmakers, regulators and accounting standards-setters are asking banks and other global institutions to turn over more data more often, and in ever-greater detail.

For many, the change will provide a shock to the system – one that has long required firms to submit static reports at regular intervals, in a standard format, year after year. The watchwords for reporting today are meaningful data assurance and granularity – they will be at the forefront of thinking for supervisors and senior bankers alike.

If there was a 'big bang' that ushered in the new era of data management and reporting, the Basel Committee on Banking Supervision (BCBS) ignited it in 2013 with the publication of BCBS 239, *Principles for effective risk data aggregation and risk reporting*. The document underscores the importance for compliance and good governance of furnishing accurate and timely data, and it has served as a jumping-off point for a host of regional and national endeavours.

Tougher all over the world

This year, the European Parliament is expected to enact updates to the Capital Requirements Directive (CRD V) and Capital Requirements Regulation (CRR II), the primary vehicles by which global standards are adopted into European law. The proposals will be among the most important regulatory developments for banks operating in the European Union in coming years and will demand in-depth analysis.

The European Central Bank's AnaCredit dataset could pose an even greater challenge because it requires an almost unheard-of attention to detail in the way firms compile data and weave it into existing credit registers. Contract-by-contract information on loans and counterparties is required, with daily updates in some countries. As if that weren't enough, the deadline for implementing International Financial Reporting Standard (IFRS) 9 is approaching, and firms also face national variations for many global and regional regulations.

Rajat Somany

Overhauls of Asia-Pacific regulation will require more frequent and detailed submissions. Broad changes are in effect or on the way for the Monetary Authority of Singapore's (MAS) 610 returns, the Economic and Financial Statistics (EFS) reporting procedures in Australia and for reports required by the Hong Kong Monetary Authority's more complicated liquidity-reporting requirements.

There has been much talk about reducing the burden on US banks, but little action, and authorities are demanding greater specificity in reports covering ordinary activities and stress-test scenarios. Credit impairment, the subject of the new current expected credit loss (CECL) accounting protocols, Federal Reserve systemic risk data (FR Y-15) and liquidity coverage are particular focuses.

Wherever an institution does business, meeting the many new or expanded requirements probably means revamping its reporting and compliance functions. High time, too, for many firms. It is still common practice in some countries to rely on manual or semi-automated data entry when preparing reports. Such methods restrict the amount that can be collected and the depth to which any analysis of it can go, and it raises the risk of inaccuracy.

That is before taking into account the abundance of information to gather, as well as the new methods by which firms will have to gather it. European institutions, for example, will have to run AnaCredit alongside such standards as financial reporting (finrep) and common reporting (corep), which heighten the likelihood of errors creeping into reports, leading to uncomfortable questions – and possibly uncomfortable fines – from the authorities. Indeed, much of the point of imposing different data collection and reporting methods is for each to serve as a check on the others to help ensure accuracy and consistency and sound management overall.

All that data and more

Regtech, with its ability to retrieve and analyse data faster, more efficiently and in greater quantities than ever, is the great hope for the industry, even if it is not clear to some just what regtech encompasses. For some vendors, regtech is a new term for technology they have been selling for years – a way to liven up the packaging without changing what is inside. A general understanding is that regtech features prodigious processing speed and storage capacity, but it is more useful than that. Collecting unprecedented volumes of

data solves one problem but creates others.

Being able to generate data down to microscopic levels only matters if it can be aggregated into meaningful packets of information that can be studied, interpreted and applied to regulatory and macroeconomic models. Regulators need accurate readings of key metrics of risk and financial performance to create a true and reliable picture of operating conditions, both current and prospective.

And regulators aren't the only ones. Bankers need the same information to manage their daily operations, to gain insight into the comparative risks and rewards of different business lines, to understand and inform risk appetite and to permit the creative, long-range planning essential to build a stronger, more profitable company. That's why the other principal features of regtech systems – agility, flexibility and an ability to be assembled on any required scale – matter at least as much as their retrieval and processing speeds, and why senior management is beginning to view investment in the technology as a worthy business proposition, and not just a way of meeting compliance obligations.

Creating and maintaining such a system requires a focus on data structure and management that permits each piece of information to be understood in the context of others – as a detail when it is necessary to consider it on its own, but also as a piece of a much larger puzzle. That, in turn, demands an approach that is at once fastidious and comprehensive – seeing the wood and the trees equally clearly – and can be applied to the design and implementation of hardware and software, and also to the service provided along the way.

This sort of approach is best achieved by a company that is simultaneously firmly rooted and light on its feet. Wolters Kluwer – with its financial wherewithal, extensive expertise in financial services and established, cutting-edge technology – is a long-standing leader in designing, maintaining and updating data management and risk management systems, and has extensive ties across the banking industry and with supervisory authorities worldwide.

Such a range of expertise is especially important today because the move to more complex, detailed reporting is just one part of a broader trend, also instigated by supervisory authorities but with commercial value as well, to integrate various functions – risk, finance, regulatory reporting – more tightly to facilitate holistic, strategic thinking that puts a greater emphasis on where business is going than on where it is now.

Firms are enlisting regtech solutions in the effort to dismantle the biggest impediment to progress in this area: a compartmentalised organisational structure that tends to lead each department to install its own system, built by a specialist supplier that has limited expertise beyond its niche. It would be a mistake to replace that antiquated technology with regtech systems purporting to be the next big thing but created in the same old way – by a small enterprise with limited understanding of the wider commercial and technological world beyond its area of specialisation.

Banks and other global institutions are being asked to turn over more data more often, in ever-greater detail

Tech of all trades

Regtech architecture permits the configuration of a system that can be scaled up and adapted to multiple uses. The traditional every-silo-for-itself alignment of technology – each producing results that were precise within its business segment and perhaps nowhere else – already carried an unacceptably high risk of generating inconsistent data; when combined with the wider variety of required reporting methods being implemented, the risks can only be multiplied.

The new supervisory order demands a data management structure that is modular, allowing it to be dropped in anywhere within a firm – for any function, at any point in its hierarchy – while being sufficiently pliable to appear to be custom-designed for each employee. The data each user produces and consumes must be co-ordinated and reconciled with the output from other departments to create a consistent, uniform picture of the business on all key criteria.

Other necessary features of regtech architecture include an ability to respond swiftly to pop quizzes from regulators, which may ask banks to provide copious data and detailed analysis of it on any subject with as little as 72 hours' notice. The agility and flexibility, plus the raw processing power, of a single overarching solution is the only effective tool to meet all these requirements.

One final capability of the most advanced systems, without which the others would be far less effective, is a user-friendly interface that permits compliance and reporting officials to see the data they need to see – not everything there is to see – while ensuring its quality and reliability. This is where state-of-the-art compliance features such as Smart Cubes come in.

An initiative of the Austrian National Bank, intended as a way for financial firms and central bankers to make sense of all the data that will be required under the Basel guidelines and the various European supervisory frameworks, Smart Cubes are standardised, automated formats for representing, validating and reporting compiled datasets. They are multidimensional matrices that permit data to be presented and interpreted more clearly, with individual items available to be reused for different purposes, ensuring greater consistency and flexibility and lower cost.

That the development of Smart Cubes was spearheaded by a central bank may seem ironic; often they are the ones that devise problems and leave it to financial institutions to find solutions. But, if the expanding reporting obligations imposed by zealously inquisitive authorities persuade institutions to overhaul their outdated systems and install fast, agile, adaptable regtech solutions that help make their businesses more efficient and profitable, then the regulators will have done them an even greater favour. ■

Contact

Frr-marketing@wolterskluwer.com
/www.wolterskluwerfs.com

Bracing for a regtech boom

With an unenviable raft of new regulation imminently coming into force, market participants anticipate a flurry of adoption of compliance-related technology, which is expected to prove lucrative for regtech providers. Joanna Wright and Max Bowie talk to some of the key players about the drivers behind this trend, and regtech's potential over the long term

The regtech – a loosely defined catch-all for providers of technology that addresses regulation and compliance issues – industry is expected to deliver impressive growth levels during 2017. That's hardly surprising, considering the amount of imminent regulation looming over financial markets participants. But what may be surprising is that providers expect a shift in the regulatory environment toward rolling incremental regulatory updates to sustain this growth long beyond the current round of regulatory issues.

The main reason for the sudden growth in regtech is the pending raft of new regulations – not least the long-awaited and already-delayed second generation of the Markets In Financial Instruments Directive (Mifid II) in Europe – and what appears to be general unpreparedness at many firms, who are now scrambling to implement solutions within much tighter time frames, and are increasingly turning to solutions providers to ensure they have systems in place before the deadlines for compliance.

The area is so active that Jim Casella, chairman and chief executive of the newly formed Compliance Solutions Strategies – which recently merged Advise Technologies, Ascendant Compliance Management and MoneyMate Group (including its Silverfinch Solvency II funds look-through data subsidiary) with backing from private equity firm CIP Capital – believes the vendor's business will grow by around 25% this year, and may also exceed 20% for the next few years.

The fact that CIP Capital chose to combine these companies – each of which served a specific aspect of compliance, but together can offer a broader offering that will serve more clients' compliance

needs via a single, integrated platform – at this particular point in time is no accident: "I had a sense that the compliance industry was going to experience significant global growth. So, over a period of time, we mapped about 150 companies and spoke to 30 before deciding that these three were best of breed and would fit together best," Casella says.

It's a similar story at Opus Global, a regtech vendor created in 2013 by private equity firm GTCR and industry veteran Douglas Bergeron with a war chest of up to $500 million to invest, which has since acquired third-party management software vendor Hiperios and know-your-customer (KYC) and anti-money laundering (AML) platform vendor Alacra.

"We saw a large opportunity to create an organisation that broad-shouldered companies can rely on, who are currently buying solutions from small vendors," says chief executive Emanuele Conti, who joined the vendor last year. "Everything we see tells us that this is a multi-billion-dollar market. There are different segments that dictate your addressable market, but we see it growing by double digits, and we don't see that abating."

But, while the new regulatory environment is creating opportunities for savvy providers, it is adding to the compliance burden of end-user firms that the vendors see fuelling their growth.

"Everybody in financial services is having to dedicate increasing amounts of time and money to regulatory compliance," says Jean White, regulatory communications manager in Northern Trust's Regulatory Solutions team, which builds regulatory solutions to help its clients comply with regulations, where appropriate – such as for compliance with Mifid II's reporting requirements, and with the European Packaged Retail and Investment Products regulation – and works with the custodian's internal compliance function. At an annual regulation conference hosted by the firm in London, a poll of attendees in 2014 showed that 50% expected to spend more time dealing with regulation over the coming year. In 2015, this number rose to 75%, and in 2016 remained high at 68% who expect to spend more time dealing with regulation this year, signalling that many firms have much left to do before Mifid II's 2018 implementation date.

Much of the challenge can be distilled into data issues, White says, such as being able to format, calculate and track data. But this already complex requirement is exacerbated if firms are still using legacy systems "that have evolved over a number of years and are not necessarily adept at handling the real-time datasets that are increasingly required."

The UK Financial Conduct Authority (FCA) has been active in fulfilling the edict of the UK government to foster the nascent regtech ecosystem. But regtech is also earning regulatory endorsement in the rest of the world, such as Asia-Pacific, says Todd Moyer, executive vice-president of global business development at Pittsburgh, Pennsylvania-based data management technology provider Confluence, citing initiatives in Hong Kong, Japan, Singapore, Australia and Canada to "create consistency and more accuracy and transparency into the data." Meanwhile, the US Securities and Exchange Commission is promoting a data strategy office to explore the potential of new data tools to support market function and compliance, he adds.

"The CRD V and CRR II proposals will be among the most important regulatory developments for banks operating in the European Union in the coming years, and will demand an in-depth analysis"

Richard Bennett, Wolters Kluwer

The sheer volume of regulation will also drive regtech further in 2017. Richard Bennett, head of regulatory reporting in Wolters Kluwer's finance, risk and reporting division, says the drivers of regtech adoption in Europe this year will be the revisions to the Capital Requirements Directive (CRD IV) and Capital Requirements Regulation (CRR). "The CRD V and CRR II proposals will be among the most important regulatory developments for banks operating in the European Union in the coming years, and will demand an in-depth analysis," he says.

Aside from the current volumes of regulation set to come into force imminently, there is a changing shift in the regulatory process that is forcing change: specifically, the ongoing churn of new regulatory initiatives expected to arise as soon as – or even before – others are complete.

"The days of having regulatory projects that are 'done' are gone. They've taken on lives of their own, which forces you to look at this for today and for tomorrow... and that's what's driving regtech," says PJ Di Giammarino, chief executive of regulatory think-tank JWG-IT. "Regtech for us is revolutionising the application of policy to the finance infrastructure... As regulators look to maintain control over an ever-changing landscape, they need to be refining those controls."

In addition, while regtech is a response to more regulation, the regulation itself is in response to firms becoming more adventurous in less regulated areas as stricter regulation in others makes them less profitable. "The more prescriptive you try to get... the more the market will adapt and try to exploit other areas of the legal code," ultimately leading these to become more heavily regulated, Di Giammarino says.

Regulation driving transformation

Besides banks, back offices in the asset management industry – which is increasingly subject to more regulatory scrutiny – are under more pressure to get data management right. Moyer says 2017 will see the beginning of a long journey to the transformation of the buy-side back office.

"Every other year at Confluence, we survey our client base, which is representative of the large asset managers and global service providers. Their number one concern for the past eight years is automating their back-office processes," Moyer says.

Those who digitise their processes further across all areas of their business will have a greater advantage. "Digitisation is cheaper and more agile, and it enables the ultimate transparency that investors are looking for. And that is what these requirements have been all about: investor transparency and understanding the underlying investments in managed pools," Moyer says. "As firms digitise, their ability to take output and use it in a more consistent and accurate fashion is going to be incredible. But that won't happen overnight."

Rory McLaren, senior vice-president of regulatory reporting services at Deutsche Börse, says that, with Mifid II looming, 2017 will be the year of implementation: "Many of the processes, tools and strategies that were previously applied to regulation are struggling to cope, and we are seeing regtech applied in a number of ways. One of these is the use of tools to help monitor and manage regulatory text. We're going to see increased use of these in the next 12 months as market participants are challenged to

"Artificial intelligence systems could be disruptive to the effectiveness of rules-based systems in monitoring behavior, for example in actively highlighting instances of market abuse. But if you can begin using machine learning to capture anomalies for regulatory purposes, you could more cleverly identify patterns" Jean White, Northern Trust

keep track of all the moving parts," McLaren says. "Semantic modelling tools could be used to better implement complex rules in a manner that makes them more visible, and easier to track and maintain by all the actors involved within an organisation."

Deutsche Börse offers such a solution, as do others such as JWG. These allow computers to model complex information obtained from regulatory documentation, and send the relevant parts of this information to applications across an organisation, looping in business, compliance and any other concerned departments. Wolters Kluwer, on the other hand, is developing its OneSumX solution into a service-oriented architecture, where a collection of connected services communicate and can operate centrally or on a distributed basis.

"Right now, the implementation strategies are really point-by-point solutions – for example, one thing for European Market Infrastructure Regulation, another thing for Mifid – and a substantial majority of the industry is in that mode," says JWG's Di Giammarino. "And all those different point solutions are causing real cost of maintenance and human capital concerns."

Confluence's Moyer echoes these concerns. "Firms realise they can no longer meet these challenges with cobbled-together point solutions or a manual process. They are beginning to look at the problem as a data problem: 'How do I manage my data?' versus 'How do I meet each individual regulation?'" he says. "Although regulations differ in what the regulatory body requires, or the actual output of the XML formats and schemas, a lot of core data is being reused across a lot of the various reports within asset management firms. So the ability to have consistent data is also very important."

And, while there may still be differences between the regulations themselves, regulators are taking a more common approach and are collaborating with other regulators and with user firms, and are utilising regtech tools to make the process of managing compliance easier for all involved. For example, Northern Trust's White says that the UK's FCA is already looking beyond just prescribing data formats for reporting, and is talking about being able to actively pull data from firms when required, which would reduce the cost of reporting for all parties involved. And this isn't the only example where new technologies could make compliance easier for end-users, but also make it easier for regulators to identify weak spots in existing regimes and draft new rules that address these areas.

"Artificial intelligence systems could be disruptive to the effectiveness of rules-based systems in monitoring behaviour, for example, in actively highlighting instances of market abuse. But, if you can begin using machine learning to capture anomalies for regulatory purposes, you could more cleverly identify patterns," White says. This could help identify areas where more regulation is needed, and ultimately lead to more efficient regulation. However, while such technologies have the potential to ease the regulatory compliance burden, they may also end up adding to it, as regulators are likely to scrutinise such tools to ensure they perform their required functions.

"Emerging technologies present opportunities to cut down on the time and effort required to meet existing regulations. But some of them, by their nature, will surely become regulated," White says. "Regulation itself isn't going anywhere. There will be advances in requirements to correspond with these new technologies, and I expect there will be regulation on how these can be utilised within financial services."

"There is no question that we see the pace of risk and regulations continuing to grow – not for the sake of creating new regulations, but because the world is evolving," says Opus' Conti. "For example, increased global trade by itself creates risk. So risks are being created by the desire to do more, and to make companies bigger and better... and, as you do those new things, it introduces more risks and attracts the interest of regulators... to ensure the risks don't outweigh the benefits."

Don't forget the data

In addition to compliance-related technologies, the specific datasets required to power regtech solutions are also expected to continue to grow in popularity and as a proportion of firms' data spend.

Douglas Taylor, founder and managing partner of Burton-Taylor International Consulting, which produces market share and industry spend reports for the market data industry and other sectors, says any datasets relating to regulation and compliance are the fastest-growing types of data.

"Anything related to pricing of complex, opaque instruments or marking portfolios to market... continues to grow, as does anything relating to AML and KYC requirements," Taylor says. Last year, Burton-Taylor predicted a five-year compound annual growth rate of 9.01% for financial markets risk and compliance-related information, and a 17.29% five-year compound annual growth rate for AML and KYC risk information. Though this year's corresponding figures will not be available until the summer, Taylor says "I'm sure the industry hit those numbers, and I expect it will do so again this year." In fact, increased spend on data to support regulation-related functions may be a key factor in the overall success of any regtech solution's implementation.

"In implementing regulatory strategies, the biggest challenge is data quality and mashing up the data, and regtech doesn't solve that – it's a classic enterprise data management problem, and involves a lot of people and processes to make it work," says Adam Honoré, chief executive of fintech advisory firm MarketsTech. "For example, banks facing Dodd-Frank requirements have the calculation capabilities that they need – it's the data quality that's the problem."

Honoré acknowledges that incremental technology advances – from the use of XBRL or the Legal Entity Identifier to regtech platforms – can yield cumulative wins, but warns that data itself remains the most important piece of the compliance puzzle: "Technology is making [dealing with regulations] easier, but it's a case of 'garbage in, garbage out'. If the data quality is not there, you can throw all the technology in the world at your problems, and it won't do a thing," he says. ■

Previously published on waterstechnology.com

Fintech and wholesale banking

Why nothing has changed

Adoption of new technologies by investment banks has stalled, leaving the industry reliant on a patchwork of fragmented, mismatched and often Heath Robinson-style software and data tools. Ian Green of eCo Financial Technology looks at the principal reasons for this lag, ranging from staff turnover to regulatory demands

Over the past decade the software industry has been revolutionised by a set of new technologies. They keep close company – where you find one you'll often find several – and the firms that have played the largest role in their creation collectively define the new economy of the twenty-first century.

These millennial technologies range from usable voice recognition and specialised storage for vast structured and unstructured datasets, to cloud computing, natural language processing, artificial intelligence and machine learning, and the rise of ubiquitous computing – meaning apps, mobile and the Internet of Things.

And yet, walking the IT floors of the large investment banks, you could easily miss the phenomenon completely. On the face of it, this seems bizarre.

Prior to the era of Google and Facebook, wholesale banking stood ahead of every other industry sector in its reliance on proprietary software engineering and invested the highest proportion of its revenues on IT. But, while there have been numerous fintech successes in retail banking – in areas such as payments and money transfers, mobile, credit and lending – equivalent successes in the more arcane world of wholesale banking are much rarer. Boston Consulting Group estimates that, of around $96 billion in venture capital funding in fintech during this millennium, only about $4 billion has been directed towards capital markets.

The investment banks are, of course, aware of the potential revolutionary nature of the millennial technologies: they have variously appointed heads of innovation and tech-savvy board advisers; set up

fintech labs and funded incubators and accelerators; directed principal investment towards fintech firms; and spawned pilot projects to experiment with at least some of the technologies such as distributed ledgers. Nonetheless, they're not actually using the technologies on a meaningful scale.

Here are five reasons for the lag:

1. The software and data estate

Given the vast scale of wholesale banks and their IT groups, and the endlessly energetic pre-crisis efforts of the banks to bring new services to clients in territories across the globe, it is no surprise now to find a legacy of thousands of applications written in an unthinkable array of programming languages deployed on a huge range of platforms at each bank. The same picture of fragmentation by accretion is true of bank data. Indeed, one of our clients that tried to classify its software assets found it had more data schemas than staff at the bank and well over 10 million lines of code for which the programming language could not even be easily determined.

While banks have evolved to be able to service such complex infrastructure, overhauling and re-platforming it on to a newer generation of technology is another matter.

On a more optimistic note, some banks have taken an entrepreneurial approach to their software estate. Given that investment in strategic systems by the large banks significantly outstrips that of even the largest software companies, a few of them have taken the sensible step of trying to monetise it (*Risk* March 2017, pages 14–18, *www.risk.net/3973736*). The motivations are various: cementing client relationships; writing down assets on the balance sheet and transferring intellectual property to a software company; funding continued development in the face of intense budget pressure; reducing run-the-bank costs; and establishing software and data standards.

If deals such as these can succeed – and, while hoped for, that remains to be seen – they will not only restore institutional pride but open a door to new multilateral models for investing in excellent software that make sense in increasingly standardised markets.

2. Business organisation versus IT organisation

Banks have historically enjoyed some signal successes in the pioneering use of technology to provide enhanced services to clients. Examples include single-dealer platforms such as Autobahn and Barx over which Deutsche Bank and Barclays – along with several peer platforms – offer a wide range of research, analysis and trade execution capabilities. We might also add Credit Suisse's Advanced Execution Services (AES), which hastened the shift towards agency execution, and, looking further back, JP Morgan's RiskMetrics, which became a standard-bearer for value-at-risk measurement and was successfully spun out into a stand-alone company.

A defining characteristic of each of these successes was close partnership between IT and the business responsible for the relevant service. The business heads had an exceptionally high degree of technical knowledge in comparison to their peers; for example, Tim Cartledge, who ran the Barx business before going on to run global spot foreign exchange trading for Barclays, was a computer science graduate. Conversely, the developers were often pulled out of the main IT areas to be seated within the business unit and sometimes given extra incentives from desk profits. In such teams, all worked together on designing the client service, framing the marketing proposition and optimising the implementation detail.

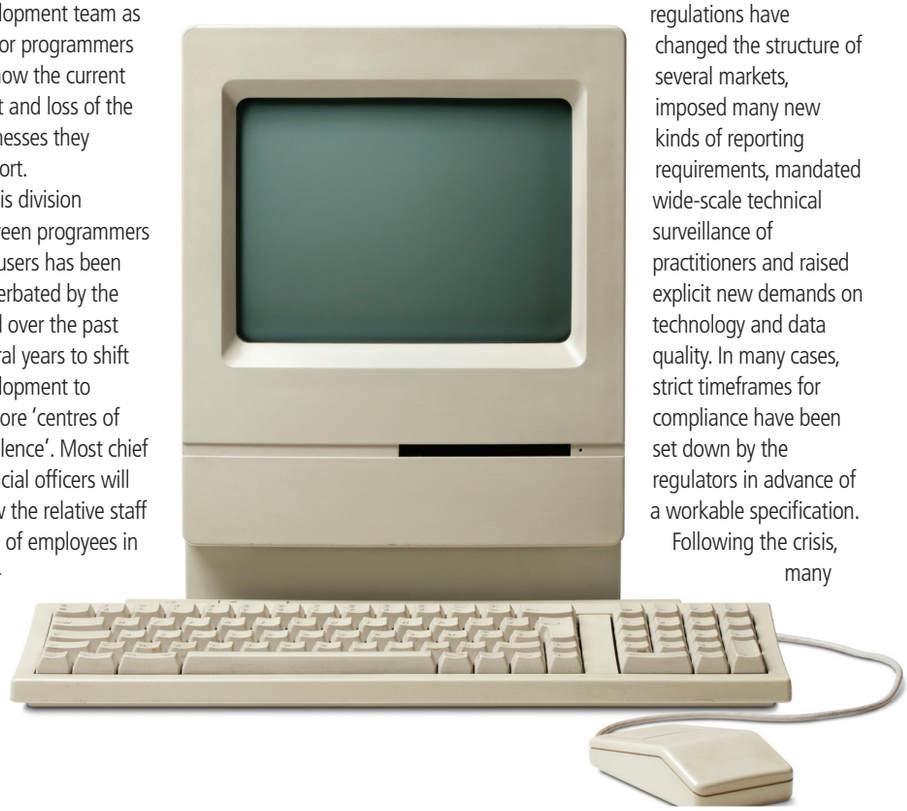
This is not standard operating procedure. For every Autobahn or AES there are literally thousands of other applications that do not receive public acclaim and are developed by programming teams that are organisationally distant from their user population. It is as rare for the users to be able to name more than a couple of members of the development team as it is for programmers to know the current profit and loss of the businesses they support.

This division between programmers and users has been exacerbated by the trend over the past several years to shift development to offshore 'centres of excellence'. Most chief financial officers will know the relative staff costs of employees in high-cost versus low-cost locations; few will know their relative code quality, even though perfectly good tools and methodologies exist to quantify it.

Without a deep unity of vision between business and IT leadership, it is virtually impossible to formulate and implement a strategy to leverage radical new technologies. Even where there is consensus on the value of these technologies, IT and business heads may have different ideas about the benefit. For some on the finance side of the large banks, making an equity investment in selected start-ups is the most natural and direct mode of participation in the fintech scene. This does not necessarily promote the use of fintech software within the investing bank; indeed, it risks the unintended consequence of distortion in the adoption of the software when the interests of the bank as an investor conflict with the interests of the bank as a client.

3. Regulation

The tsunami of regulations following the 2008 crash has affected IT just as much as every other department of the large investment banks. Firstly, there is the direct impact on the appetite for IT investment of enormous fines and compliance costs coincident with a halving of fixed-income revenues. More even than this, the need to comply with regulations such as the *Fundamental review of the trading book* (FRTB) and Europe's revised Markets in Financial Instruments Directive (Mifid II) creates massive new work programmes for IT. These regulations have changed the structure of several markets, imposed many new kinds of reporting requirements, mandated wide-scale technical surveillance of practitioners and raised explicit new demands on technology and data quality. In many cases, strict timeframes for compliance have been set down by the regulators in advance of a workable specification.



Following the crisis, many

banks announced ambitious targets for IT cost-cutting, but this was rarely achieved. Instead, IT budgets tended to flatten out at the start of this decade and all available IT resource was channelled to regulatory initiatives, virtually eliminating the capacity to do anything other than keep the lights on and comply with new laws. Most commentators who estimate IT spending now report rises over the past couple of years that are set to continue; this spending remains dominated by conformance to regulatory initiatives and associated market changes.

In principle, some of the millennial technologies appear suitable for use in meeting some of the new regulatory requirements. However, the precarious nature of the banks' software and data estate, the lack of time and money to incorporate research and development into the delivery pipeline, and the combination of tight deadlines and uncertain regulatory specifications all conspire against thoughtful IT strategising.

4. Partner engagement

Given that all banks need to transform the way they operate at the same time to comply with the same regulatory changes, an obvious idea presents itself: rather than each bank bearing the full cost of their necessary change programmes, couldn't they mutualise the cost through collaboration initiatives and/or increased use of third-party software? While we believe this will ultimately come to pass, it has not happened yet on a significant scale.

To understand why, we need to comprehend how banks engage with vendors, how banks engage with each other and how banks, in IT terms, think of themselves.

Taking the last point first, we have seen that IT heads find themselves responsible for software and data estates of boggling complexity, with no time to research new technologies or collaboration plays that may improve active project outcomes and with forbidding compliance deadlines set down in law. It is, perhaps, a fact of psychology that the more deeply you feel yourself to be lost in a byzantine wormhole, the harder it is to recognise it as a shared plight that may be addressable by social strategies. Accordingly, senior technologists with accountability for meeting, say, a key Mifid II date are reluctant to let a day pass in which they do not take a step forward from their particular form of darkness into a state that may be adequately light. In this context, collaboration initiatives can feel like an irrelevance or even a distraction.

Historically, the largest banks – as opposed, say, to regional banks – have had a patchy experience with third-party software. In part, the difficulty stems from the same issue: the first priority of the bank is to husband its proprietary tech stack, and the adoption of alien standards, interfaces or design patterns comes a poor second. Even when banks license third-party software, their integration and deployment processes – the purpose of which are to keep the bank's current Jenga tower intact – frequently impair its proper use.

IT budgets tended to flatten out at the start of this decade and all available IT resource was channelled to regulatory initiatives, virtually eliminating the capacity to do anything other than keep the lights on and comply with new laws

This aside, it is notoriously tough for a software company to negotiate with an entity whose IT, business and procurement departments are often individually powerful, organisationally distant and misaligned. With few exceptions, software companies often simply give up and look for more attainable revenues from smaller banks and buy-side firms that are more proficient at licensing software.

It is worth noting that millennial technology is often available as open source software (OSS). This has not normally been true of software from the vendors that serve banks. The ensuing lack of transparency has tended to make implementations harder and engender mistrust. Unfortunately, banks do not generally play a full and healthy role in OSS communities. While all developers use OSS, policy and legal restrictions and security concerns at banks make it harder to download and evaluate, and also block normal code contribution practices.

The consequence is that banks tend to have something along the lines of a "don't ask, don't tell" policy to OSS in which they make hundreds of thousands of downloads but then need to maintain their own versions of it all rather than checking changes back into the public code line. As well as impairing the natural role of talented developers as good OSS citizens, this is costly and quality-reducing. If this can be fixed, it will enable banks to develop higher-quality, more functional relationships with alternative software suppliers and, potentially, with each other.

The relationship of the banks to each other may ultimately be the most subtle and important factor that affects technology transformation. We still encounter senior staff inside and outside IT who hang on to the idea of technology differentiation and believe their anti-money laundering system or their special flavour of data lake will confer a competitive edge. Much more often these days we find staff who are almost overwhelmed by the forbidding difficulty of delivering core projects that are either critically underfunded or, more rarely, staffed to an unmanageable degree out of regulatory panic. Between the two there are occasional calm heads creatively seeking a path of rational co-operation with peer banks and other external parties. For these people, the twin challenge is to find fruitful collaboration paths outside their firms and to establish traction within. If initiatives with, say, blockchain or cyber security or fraud detection achieve significant success over the coming years it will be down to them.

5. Staff turnover

The single greatest obstacle to collaboration initiatives and the alignment of software and business goals is turnover among decision-makers at the banks. The visionaries who might develop, nurture and promote great new practices don't stand much chance when they and their management are frequently reshuffled. Heads of innovation come and go even more often than chief information officers: in a spot check of nine heads of innovation for this article, only one had been in place in 2015.

Whether this indicates dissatisfaction of the staff themselves or of their employers or of both is hard to gauge; most probably it reflects a sense of mutual frustration arising from the chasm between the blue-sky tech strategists and the developers who run production systems.

For strategic progress to be sustained, the pace of turnover of critical staff needs to slow. Tenure in roles is required for the more thoughtful staff to find and connect with each other and start to change things. ■

Previously published on Risk.net

Ian Green is chief executive of eCo Financial Technology, which he co-founded in 2014. He previously worked at Credit Suisse as global head of fixed income e-commerce. Ian can be contacted at: ian@ecofinancialtechnology.com

Mifid malfunction

Brexit breaks data foundations

Removing the UK from EU markets could derail new European trading and transparency rules. By Samuel Wilkes, with additional reporting by Roberto Barras

Need to know

- The second Markets in Financial Instruments Directive (Mifid II) and Markets in Financial Instruments Regulation (Mifir) will apply in the European Union from January 2018.
- The rules contain numerous running calculations and assessments that determine which requirements apply to which instruments and market participants.
- These calibrations affect rules such as the determination of systematic internalisers, pre- and post-trade transparency, caps on the use of equity dark pools, and the regulation of commodity trading.
- Due to the large share of trading volume transacted in the UK, removing UK data from those assessments after Brexit will have unpredictable effects on their outcome, potentially rendering some impractical.
- To recalibrate the thresholds, the European Securities and Markets Authority will have to be empowered by the European Commission or wait until 2021 for a scheduled review of the rules on non-equity instruments.

For most of the past decade, legislators in Europe have been carefully crafting the vast construct that is the second Markets in Financial Instruments Directive (Mifid II) and its accompanying Markets in Financial Instruments Regulation (Mifir). Once Mifid II takes effect in January 2018, its requirements are designed to alter over time, in keeping with the gradual changes in the size and shape of European Union markets.

At the heart of this calibration process is the data underpinning Mifid II's regulation of market structures and practices. If this crucial reference dataset were to be altered dramatically, it would completely distort the functioning of many central planks of Mifid, including trading and transparency obligations for equity and non-equity instruments alike.

Enter Brexit. If the UK were to leave the European Economic Area (EEA) single market without a post-Brexit special arrangement, trading activity in the country would no longer count towards assessments used within Mifid II. The London markets account for a vast proportion of total trading activity in the EU, from around 30% of equity dark pool volumes to as much as 80% of interest rate swaps.

As thresholds have been set with the UK in mind, the sudden removal of that data means assessments become either defunct or false after Brexit. This could force a significant review of Mifid II in 2019, although there is no official legislative review for non-equity instruments scheduled until 2021.

"When you start to think about the implications of Brexit on Mifid II, you think, 'Dear God, look at all this stuff we have to think through.' Of course, nowadays everyone is just focusing on the two or three fires that are directly in front of us and not looking down the line to see the big one coming in over 24 months," says Nathaniel Lalone, a partner at law firm Katten Muchin Rosenman, based in London.

Mifid II and Mifir will apply to EU markets from January 2018. As the UK will still be part of the union in 2018, Mifid II will apply to UK markets at the launch date.

The UK government triggered Article 50 – the mechanism for leaving the EU – in March. Unless extended by agreement with the remaining 27 members of the EU, the Article 50 process for leaving the union will expire at the end of two years. At that point, the UK would no longer be classed as an EU market and would no longer contribute to EU data. The expectation is that the total size of the EU-wide market will dramatically shrink to the point where some Mifid requirements will not function properly.

"You can get into the detail of Mifid II and find quite a number of areas that will be affected by Brexit, and I think the biggest one is going to be the transparency calibrations," says Matthew Coupe, a director in market structure at Barclays. "You suddenly find, based off the UK leaving the EU and therefore dropping out of that data, the thresholds are completely out of alignment and therefore would need to be recalibrated."

Distorting thresholds

Within Mifid II, there are pre- and post-trade transparency requirements for non-equity instruments. If a product is subject to these rules, venues and firms will have to publish bids and offers on a trade before execution, as well as the price and size of the trade immediately afterwards.

To determine which products should be allowed a waiver from these requirements there is a liquid market test. If an instrument is found to have been traded infrequently relative to its asset class, it is classed as illiquid and a waiver can be applied to transparency requirements.

The liquid market thresholds were calibrated by the European Securities and Markets Authority (Esma), based on EU-wide repository data, which included the UK. The assumption is that if the UK no longer counted towards the total EU trading activity, then those thresholds would no longer be appropriate. For example, fewer bonds would meet the requirement in the liquid markets test to trade a minimum number of times per day.

"If you remove the UK from the equation, the thresholds are possibly then set too high because of the outsized amount of liquidity that is concentrated in London. There is an argument to be said that the act of Brexit could or should be a reason for looking at these thresholds and seeing if, in a post-Brexit world, they still make sense," says Lalone at Katten Muchin.

Fragmenting liquidity

The calibration of the trading obligation for non-equities could also be affected by Brexit, as it would significantly alter the data used to determine which instruments should be traded on EU venues.

The trading obligation is one of the Group of 20 commitments agreed at Pittsburgh in 2009. Over-the-counter derivatives captured under the obligation will only be traded on platforms. To be subject to the obligation, a class of derivatives must be subject to the clearing obligation, be deemed 'sufficiently liquid' and pass a venue test.

In a discussion paper published on September 20, 2016, Esma proposed a series of thresholds that would be used to determine which cleared derivatives are sufficiently liquid to trade on-venue. This included the number of trades per day, average notional per day, days traded and the number of distinct counterparties.

The thresholds were calibrated based on EU-wide repository data. Without a special arrangement after Brexit, the data fed into the calculations would be a false reflection of EU trading.

Francis Todd, a managing director in the securities division at Goldman Sachs, told the audience at a conference on derivatives trading, organised by the International Swaps and Derivatives Association in London, in December last year: "One obvious thought is if London does slip away and the UK falls outside the EEA, then all of the trading activity done in the UK would not contribute towards the calibration of the test, at least after it takes effect. So that may cause the calibration threshold to have to be thought through."

"You suddenly find, based off the UK leaving the EU, and therefore dropping out of that data, the thresholds are out of alignment"

Matthew Coupe, Barclays

According to data compiled by the Bank for International Settlements, more than 80% of over-the-counter interest rate derivatives trading in the EU takes place in the UK.

The pre-Brexit dataset for sterling interest rate swaps would be particularly misleading, as trading takes place almost exclusively in London, and one source says EU trading of dollar swaps is similarly UK-dominated. In its September 2016 discussion paper, Esma outlines three tenor dates for sterling and eight for dollar interest rate derivatives, which would be subject to the trading obligation.

Esma does have the ability to recalibrate the trading obligation. If there is a "material" change to the liquidity of those derivatives subject to the trading obligation, Esma can revoke, suspend or amend the regulatory technical standards.

"The question is really: does the liquidity pool fragment? If it does, what does that mean? The European dataset only covers business done in a particular product within a defined region, rather than looking at the product's liquidity profile, regardless of where it's traded. So already it does not include a substantial amount of trades executed on-Sef [swap execution facility] under US rules. The fragmentation may cause a change in liquidity, and then you would question whether the thresholds are still the right ones and would they revise them anyway?" asks Simon Maisey, managing director of fixed-income and swaps multilateral trading facility Tradeweb in London.

Smaller SIs

The disruption caused by Brexit to the inner workings of Mifid II will not only hit trading on multilateral venues; the damage extends to bilateral trading governed by the systematic internaliser (SI) regime.

The SI designation is a unique status assigned to dealers under Mifid II if they trade a large amount of an instrument outside of a venue. The designation is based on passing a market-share threshold applied to each sub-asset class. For OTC derivatives with a liquid market, if a dealer trades more than 2.5% of the total number of transactions executed in the EU in a class of derivatives, they are deemed an SI.

Dealers are not particularly welcoming of SI status, as it comes with a series of transparency and reporting obligations to fulfil, including providing firm quotes to the entire market.

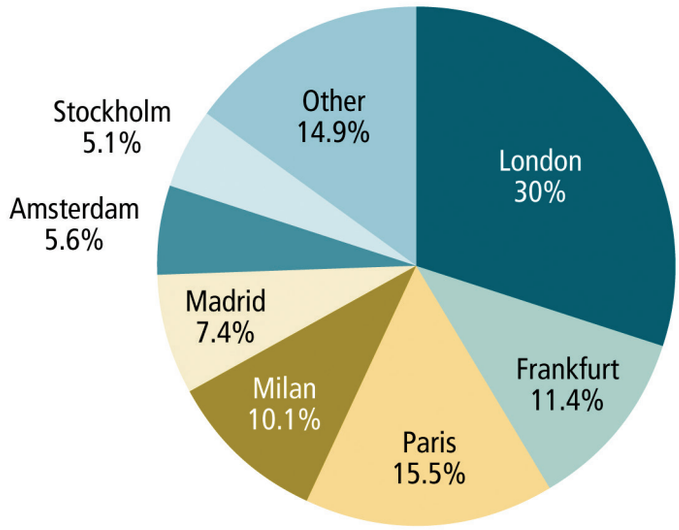
If the thresholds remain the same, Brexit could cause the SI bar to lower dramatically, because the total market size would shrink – resulting in smaller EU firms suddenly becoming SIs.

"Once you take UK trading activity out of the SI calculation equation, then an investment firm in the EU that might not have been an SI in an instrument, or class of instruments, before Brexit [based on threshold calculations] could become a much more significant player in relative terms, precisely because the UK trading data drops out of the EU-wide denominated data," says Daniel Csefalvay, a partner at law firm Linklaters, based in London.

Smaller firms might not be ready to manage the market and operational risks generated by the SI obligations. One source says Brexit could also make the SI assessment more volatile as firms undertake episodic hedging programmes, depending on their business; for example, bond houses carrying out an interest rate-hedging programme. With a smaller market size, such specific and temporary programmes could throw a firm over the threshold, obliging them to keep a permanent presence in the market for at least three months until the next SI determination date.

But an alternative possibility, points out Coupe at Barclays, is that there could be fewer SIs. "If a firm is not operating within the EU, then you will have a reduction in the number of SIs. But it depends on how much of the current flow of trading in Europe would move into the EU or stay in the UK," he says.

1. Market distribution of Bats Europe dark order books (% of EEA trading, as of February 6, 2017)



EEA = European Economic Area. Source: Bats Europe

Dark pools get murkier

Equity instruments are also subject to a trading obligation under Mifir, although this works differently from the requirements for non-equities. For equities, there is a double-volume cap mechanism on the proportion of trading that can take place on venues where traders can operate anonymously. This regulation of so-called dark pools would be affected by Brexit.

The first cap is 4% of the total volume in one stock being traded on one dark pool for a period of 12 months. The second limit is 8% of the total volume of a stock being traded on all EU dark pools for a 12-month period.

Depending on the limit an individual stock breaches, either an individual dark pool has to suspend trading in that stock – for the 4% cap – or all EU dark pools must suspend trading in the stock – for the 8% cap – for six months. It is uncertain how the UK leaving the EU could affect the double-volume cap mechanism for the EU, as the total breakdown of EU volumes is not yet known. The data is not publicly available, but should be once Mifid II is live.

"There is uncertainty [over] what the impact of double-volume caps will be, [even] before thinking about Brexit. Maybe the volume caps don't have any impact across foreign dark pools because European trading might not be so large and there is no need to trade in other regions. Or firms might find themselves very restricted in Europe, and might want to look at the US and Switzerland, but that is uncertain at the moment because we don't have the right data," says Christian Voigt, a senior regulatory adviser at trading technology firm Fidessa in London.

One expectation is that, following Brexit, there would be further room for dark pool trading in Europe, as a lot of existing dark pool trading in European stocks is booked in London (see figure 1).

"Quite a lot of the calculations for double-volume caps will be based on London data. As soon as you [have] Brexit, unless something is put in place to continue to capture London data, then suddenly, the double-volume cap issue for stocks becomes less of a problem in Europe," says Tim Cant, a senior associate in financial regulation at law firm Ashurst.

It could, however, have the opposite effect and further restrict dark pool trading in Europe. This would result if the total amount of lit stock trading in the EU decreases, but the threshold remains the same.

"You could calculate, once the UK departs from the EU, the denominator becomes much smaller for the volume calculation because you have taken a substantive amount of trading out of the picture," says Juan Pablo Urrutia, European general counsel at dark pool operator ITG.

Moreover, if UK dark pools fail to obtain an equivalence determination from the EU, any stocks traded in the union could not be traded in London by Mifid-registered firms. Several UK-based dark pool operators are apparently looking at setting up entities in Dublin to ensure continuity of service to their EU participants.

If the UK wants to maintain equivalence with Mifid II, then the domestic regulation will have to look similar to Mifir, even after Brexit. But it is unclear whether the double-volume caps would necessarily have to be in UK law.

"Unless they needed the double-volume caps [for UK-based firms] to acquire rights to a Mifid II passport, I doubt the FCA [UK Financial Conduct Authority] would apply the caps out of its own will. I don't believe the UK was ever in favour of the double-volume caps," says Urrutia.

Within the Mifir rules for equivalence there is no mention that the determination is dependent on either the double-volume caps or market structure more generally. If the UK was to apply its own double-volume cap mechanism, this could severely limit the amount of dark pool trading in the UK.

"If the UK was unilaterally applying a cap at that point in time, it would be difficult to know how many broker dark pools will continue. In an odd scenario, we could end up being the sole major dark book in the UK. Then we would be measuring against ourselves and at that point it might become a nonsense," says Adam Eades, chief legal and regulatory officer at Bats Europe.

> "If you remove the UK from the equation, the thresholds are possibly then set too high because of the outsized amount of liquidity concentrated in London" Nathaniel Lalone, Katten Muchin Rosenman

Esma and the European Commission do have several options available to them when it comes to recalibrating the Mifid thresholds. But the solutions don't come without challenges and none provides an overnight fix.

Can they fix it?

Within the Mifir level-one legislative text are provisions for reports and reviews of the regulation,

including the transparency waivers and double-volume cap mechanism.

Article 52(1) of Mifir states that the European Commission, in consultation with Esma, shall provide the European Parliament and Council of the EU with a report on the impact of the transparency obligations and the double-volume cap mechanism by March 3, 2019. This is to include feedback on the "continued appropriateness of the waivers to pre-trade transparency obligations".

"[This report] could serve as an independent – and, as regards Brexit, timely – trigger to re-evaluate the transparency regime, including thresholds, through amendments to the level one text," says Lalone of Katten Muchin.

Esma also has the ability to tighten the threshold for bond markets, but only up to a predetermined limit set by the European Commission, and only after an annual impact assessment, which would potentially complicate the implementation schedule for any changes.

Moreover, there is no guarantee that the Article 52(1) review process could be carried out in a timely fashion. A review of the European Market Infrastructure Regulation (Emir) began in 2015, but the European Commission has yet to publish an actual legislative proposal.

If there were to be a recalibration of the thresholds, at least the introduction of Mifid II would provide Esma with better quality data from 2018. The regulator could then use that data to determine the location of trading activity and assess the impact of Brexit on the transparency rules.

"I think it wouldn't be that complicated, because Brexit would happen post Mifid taking effect. When Mifid comes in, there is going to be a lot more reporting, both to the public and regulators. One of the challenges Esma has had in the past is gathering accurate data. Making any changes post-Mifid means they will have a more accurate dataset," says Maisey of Tradeweb.

"We could end up being the sole major dark book in the UK. Then we would be measuring against ourselves and it might become a nonsense" Adam Eades, Bats Europe

But others doubt whether it would be so simple for Esma to recalibrate the thresholds, especially if it was only granted the powers to begin doing so in 2019.

To be able to determine how much Mifid-regulated trading takes place in London, Esma would have to request not only the trade reports, but also every single EU firm's individual identifier, from an approved publication arrangement (APA). An APA is a vendor that is authorised to publish trade reports on behalf of investment firms. As APAs do not usually identify individual counterparties in their trade reports, Esma will need a special arrangement to ensure this extra information is provided.

Moreover, as Brexit unfolds, there is an expectation that some firms will start shifting their activity out of London, potentially into the rest of the EU – generating further changes to the data used by Esma to calibrate the thresholds.

Most dealers operate a centralised booking model, where they book their trades from across the globe in one location. For many, that location is London. Brexit is already prompting banks with large Asia-Pacific trading operations to consider setting up local booking hubs rather than backing trades into London.

"The data would already be there, because we will be live and we'll have post-trade transparency data. So the conversation of where the thresholds should be set should hopefully be less complicated," says Coupe. "Nevertheless, I'm sure it will still be complicated because we will need to start filtering out what is different between a European trade and a UK trade, and how that structure works. That will depend on how firms organise themselves in the new world." ■

Previously published on Risk.net

Additional reporting by Philip Alexander

TESTING TIMES FOR ANCILLARY BUSINESS

One of the most dramatic changes ushered in by Mifid II is the expanded reach of financial regulation to cover commodities trading. The distorted dataset after Brexit could bring far more energy firms under the auspices of Mifid II rules, such as commodity position limits and reporting obligations.

Under Mifid II, energy firms can avoid the regulation by invoking an 'ancillary business exemption', designed to exclude companies for which commodity trading is an incidental activity rather than part of their core business.

To obtain this exemption, energy firms must pass a two-part test. A firm has to identify all of its trades that are included in the scope of Mifid II, known as non-privileged activity.

For the exemption, firms first need to calculate their non-privileged trading activity as a percentage of their main business activity, as measured by gross notional value. The outcome of this calculation determines the amount of market share firms are allocated in the second part of the test, known as the market share test.

The market share a firm is allowed depends on whether its non-privileged activity is less than 10%, between 10% and 49.9%, or 50% or greater of its total business activity. The market share test has to be conducted for different commodity asset classes – oil, natural gas, power, coal, freight, emissions and metals – each with different market share allowances. Should a company fail the two-part test, it will still be able to fall back on a capital examination to demonstrate its trading activity is ancillary to the core business.

The main business test will not be affected by Brexit, but the market share test certainly will. As UK trading contributes a significant size of the market share of most of these asset classes, the bar for EU energy firms to breach would be lower post-Brexit. This will potentially capture more EU energy firms under Mifid II.

"The UK market is going to make up a large proportion of the EU's market size, and the UK leaving is going to have quite a big impact on those [EU] companies that are currently just below the threshold," says Owen Williams, a London-based associate at law firm Clyde & Co.

Banks test blockchain potential

Regulators can monitor a million active trades and hundreds of messages per second in swap test. By Luke Clancy

A group of banks and tech firms has tested the use of blockchain technology and smart contracts for the affirmation and post-trade lifecycle management of equity swaps, in concert with a node on the network acting as a regulator to test the technology's potential to allow for real-time market surveillance.

A group of banks and tech firms has tested the use of blockchain technology and smart contracts for the affirmation and post-trade lifecycle management of equity swaps, in concert with a node on the network acting as a regulator to test the technology's potential to allow for real-time market surveillance.

The test – on over-the-counter single-name, total return, index and portfolio equity swaps – was conducted by a group of five banks and organised by distributed ledger technology (DLT) firm Axoni.

The banks involved included Barclays, Citi, Credit Suisse and JP Morgan, with vendor IHS Markit inputting trade confirmations, Thomson Reuters piping in data and consultant Capco interacting as a non-dealer buy-side node on the DLT network. Capco's primary role, however, was to provide supplementary consulting on market structure.

Axoni also sought to test the privacy of parties involved in the transactions, adding and removing permissions for participants, establishing access to data, throughput, analytics and data queries. It was proved that a third party, acting as a regulator, could be given full access to see the entire market and "pull out very complex analytics", says Axoni chief executive Greg Schvey.

The regulator node viewed more than a million active trades and processed hundreds of messages per second in real time. This enabled it to monitor systemic risk while preserving data privacy between trading counterparties.

"Regulators want to fulfil objectives related to quality and transparency of data. In equity swaps, we've taken an extremely fragmented market structure and delivered a system-wide view with fully accurate data in real time," says Schvey.

In September 2016, the participants in the proof-of-concept test of Axoni Core, Axoni's proprietary distributed ledger software, conducted a diverse set of 133 test cases within the lifecycle of swap contracts. For example, two different ways to create a trade were tested: smart contracts were generated from simulated legal confirmations sourced from trade-processing platform MarkitSERV or trades submitted by counterparties on the distributed network, resulting in a synchronised, golden record of each transaction.

In a permissioned, distributed, peer-to-peer blockchain network, the initiative processed post-trade events inherent to equity swaps, including mark-to-market calculations, margin calculations, payments, corporate action processing, novations, extensions, updates to economic terms, updates to reset dates and terminations.

Thomson Reuters provided data feeds through its DataScope product by integrating with Axoni software, which enabled the input of reference data, corporate actions, Libor rates, entity data, end-of-day pricing and evaluated pricing services directly on the blockchain. This enabled the smart contracts to automate workflows, including accrual calculations and eventually simulated payments and margin.

Real money was not transferred, but payment values were calculated and synchronised across parties so they could be plugged into a real-world payment system, and subsequently referenced against the shared record on the blockchain, says Schvey.

Not all corporate actions were tested, but it was proven that an external signal could automate functions on the smart contracts such that both parties processed them synchronously. Likewise, the smart contracts did not attempt to deal with tax accounting.

Given both parties to the trade are executing the code synchronously and co-processing the transactions, it should be easier to resolve disputes transparently, Schvey adds.

Cost saving and op risk reduction

"The proof-of-concept has shown that blockchain technology lends itself well to solving the operational complexity and volumes of equity swaps lifecycle processing," says Roman Eisenberg, global head of prime services technology at Credit Suisse. "This can possibly present an opportunity to not only save costs but also reduce operational risks while growing the client offering."

Schvey says further market buy-in is essential for widespread adoption of the technology, and Axoni is talking with a variety of firms to join the project: "The world of equity swaps can be broken down into consumable chunks, and we are focusing with firms on what parts they can get up and running quickly and built on from there."

Axoni says it is also working in credit derivatives, foreign exchange spot and forwards contracts, and believes the same technology can be used to improve post-trade asset servicing in these products.

Separately, Axoni is looking into reference data challenges, working jointly with blockchain company R3, banks and the Securities Industry and Financial Markets Association to create a proof-of-concept. Reference data makes up 40% to 70% of the data used in financial transactions, and includes information such as financial product specification, issuer detail, counterparty information, currencies, corporate actions and prices.

Reference data requires constant maintenance, as reference entity names, counterparties and securities data change over time.

Rationalising further use cases

In April 2016, Barclays Investment Bank demonstrated a proof-of-concept for interest rate swaps smart contracts, which provided an end-to-end vision ranging from standards bodies providing templates for smart legal agreements to banks executing the resulting smart contracts on a distributed ledger. This included leveraging International Swaps and Derivatives Association agreements and running smart contracts on R3's prototype Corda platform.

Barclays subsequently highlighted its interest in experimenting with equity smart contracts as well, so was keen to participate in Axoni's collaborative testing of equity swaps smart contracts.

Lee Braine, who works in Barclays' chief technology office, says: "Much of this proof-of-concepting and experimentation across the industry of blockchain concepts helps to mature both the technology and our understanding of the potential applications of it. And this includes the ongoing process of rationalising the many candidate use cases down to a shorter list of potentially viable business cases." ■

Previously published on Risk.net

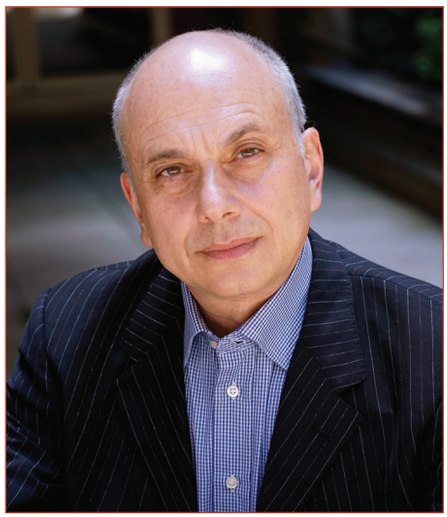
Blockchain: a solution looking for a problem

While new financial technologies show much promise, many proposed applications are naive or miss the mark, says Alexander Lipton

Fintech in general – and blockchain and distributed ledger technology (DLT) in particular – are currently the toast of the town. Expectations of their impact on the banking industry are nothing short of miraculous; it looks like finance is going through a 'cold fusion' phase. Potentially, fintech can have numerous applications; as of now, it is not clear which ones.

Although the current obsession with blockchain and DLT is inspired by Satoshi Nakamoto's 2009 tour de force, *Bitcoin: A peer-to-peer electronic cash system*, bitcoin is not the first digital currency and very likely not the last one either.

There are multiple historical examples of blockchains and distributed ledgers. For instance, family trees of ruling dynasties are blockchains. Moreover, since they were independently maintained in several capitals, they also represent distributed ledgers. More recently, we've seen digicash invented by David Chaum in the 1980s, and Bit Gold invented by Nick Szabo in the 1990s.



Alexander Lipton is a Connection Science Fellow at MIT and an Adjunct Professor of Mathematics at NYU

While all the building blocks of bitcoin have been known for some time, their unique combination captured the public's imagination only recently. In the beginning, bitcoin's appeal was strong, especially given justifiable disenchantment with the banking sector. It was expected to be a viable non-inflationary peer-to-peer currency based on a proof-of-work unpermissioned public ledger.[1]

Reality proved to be less glamorous. Bitcoin supports about seven transactions per second, with real transaction costs of approximately 1.5%. This is down from 2012, when costs were a whopping 8%.[2]

Anecdotally, bitcoin consumes as much electricity as eBay, Facebook and Google combined, making mining a cost-of-electricity game. The environmental costs of bitcoin, which are frequently ignored, are obviously huge. Additionally, bitcoin uses an archaic single-rather than double-entry accounting system.

Bitcoin miners coalesce in gigantic pools, with the three largest pools responsible for about two-thirds of all the work; thus, collusion among these pools makes a 51% attack possible, with the aggressor being able to revise a transaction history, or prevent new transactions from confirming.

Currently, rather than a worldwide distributed system, bitcoin is highly centralised and predominantly orientated towards the Chinese market. In the words of a Russian ex-prime minister, Viktor Chernomyrdin, "we wanted the best, but it turned out as always".

Another problem to be addressed is the sheer scale of the global economy, which precludes the use of an unpermissioned public ledger such as bitcoin. This has led to permissioned public ledgers such as Ripple, and private ledgers such as those run by R3, IBM and Digital Asset Holdings, being proposed as alternatives. That is not to say it is impossible to use DLT to good effect. Inspiration for its use comes from the Estonian experience of switching to a digital government, which was accomplished by connecting all important databases via an adaptor called the X-road.

A similar concept can be used to link financial institutions via DLT. The financial X-road has to be a permissioned ledger, controlled by trusted notaries paid for their services. Two financial institutions use their respective adaptors to agree on a transaction, execute it via a smart contract, then secure it by hashing. Afterwards, a quorum of notaries digitally signs the hash and posts it in the common layer, creating an immutable public record – 'laminating' the transaction, in other words. It is imperative that both securities and cash are treated on a par.

One of the juicier targets is the holy trinity of capitalism – trading, clearance and settlement. DLT is clearly unsuitable for high-frequency trading, since distributed clocks are not truly synchronised. However, permissioned private ledgers can certainly cut costs, speed up clearing and settlement, and reduce the burden of reconciliation and failures. Yet, the instantaneous settlement – or T+15 minutes as it is occasionally called – should not be implemented, because it obliterates pillars of the current system such as netting, stock borrowing and anonymity.

There are several other areas where DLT can be useful. Trade finance, syndicated loans and other similar high-friction areas are additional attractive candidates for DLT. In global payments, the potential to use DLT is also relatively high. However, despite statements to the contrary, the existing payment system is expensive but not broken, so competition will be tough.

So although the idea of a blockchain and DLT is not novel, modern technology gives it a new life. It remains to be seen where its applications will be best served, however. ■

Previously published on Risk.net

[1] *The total number of bitcoins in circulation is now 21 million, 16 million of which have been mined and 3–5 million potentially irretrievably lost.*
[2] *Claims that bitcoin can solve the issue of half the world's population being unbanked are simply ludicrous.*

ORACLE Deloitte.

Compliance to Competitive Advantage:

Leveraging Regulatory Data for Strategic Insight

Oracle and Deloitte surveyed 275 North American C-level and senior executives from financial services organizations to explore how they can more effectively leverage regulatory data to drive their business forward.

USING DATA FOR COMPLIANCE VS. COMPETITIVE ADVANTAGE

A Missed Opportunity: Data for compliance reporting is NOT leveraged to derive strategic insight.

66% say their data strategy is more effective at complying with **regulatory requirements** than **driving the business** forward.

UNTAPPED OPPORTUNITIES AHEAD

- Executives report that, if they could successfully leverage regulatory data for strategic business decisions, they could drive a **12%** increase in annual revenue.
- **For an institution with $1 billion in annual revenue, that's an additional $120 million each year in revenue.**

EVOLVING REGULATORY REPORTING NEEDS

Top Priorities for Improving Regulatory Reporting Capabilities.

#1	**Develop a framework for managing data used for various internal needs and external reporting.**	**59%**
#2	**Automate end-to-end reporting process from data aggregation to submission.**	**57%**

Financial organizations are looking to get ahead by using business insight obtained from data to drive growth and profitability. Speak to Oracle to learn how you can take action, to avoid missing the mark.

For more information:
Website: www.oracle.com/industries/financial-services
Email: financialservices_ww@oracle.com