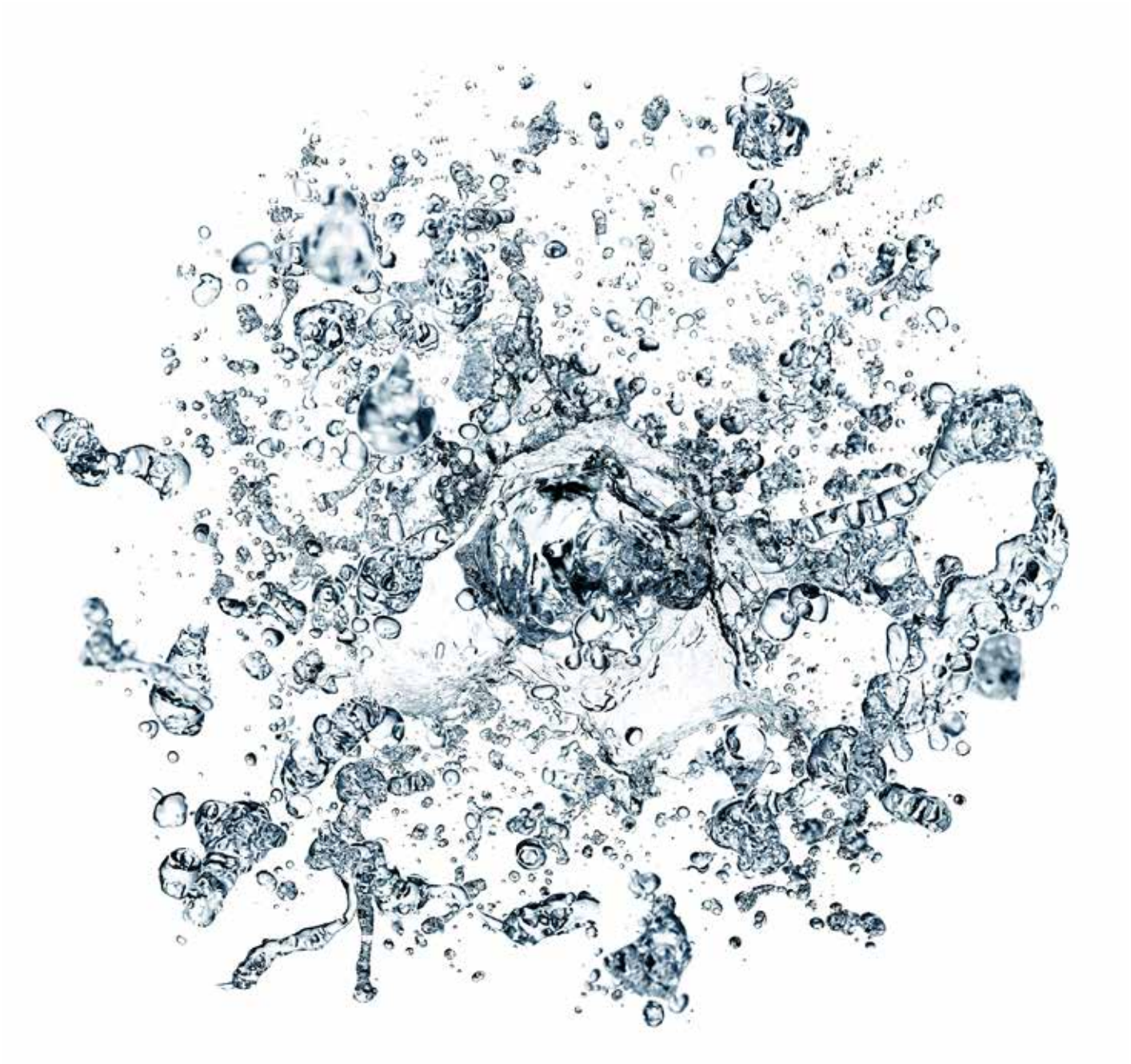
FSI*Review*

Deloitte Southeast Asia
Financial Services Newsletter
Issue 18, August 2018

The changing world of technology in financial services

- New tech and FinTech: Embracing the opportunity and grasping the risk
- The state of cyber security at financial institutions
- Trade-based money laundering compliance: A balancing act
- The EU Benchmark Regulation and practical implications of the third country regime



Deloitte.

Making a splash

Over the last six months, technology and innovation continue to dominate regulatory discourse across Southeast Asia. In Malaysia and Singapore, the evolution of payments in response to new technologies is a subject of interest for industry players. Financial institutions and regulators understand the impact of artificial intelligence, blockchain and other new technologies, which have the potential to fundamentally change how financial institutions run their businesses and how their customers borrow, save, pay, invest or insure.

Banks, insurers and investment management firms have begun harnessing exciting new digital technologies to improve efficiency and better service their clients. However, the use of these technologies come with a price: generating risk at multiple levels, which will require adapted response and control. Our first article looks at blockchain and discusses the possible risks that come with embracing these technologies.

Cyber threats and attacks are growing in both number and complexity. Implementing a cyber risk management plan is paramount to protecting a financial institution's business. How do these firms measure success with cyber security? We take a closer look at a recent Deloitte survey examining how firms develop and deploy best practices.

Trade finance has regularly been seen as a "higher risk" business for money laundering, terrorist financing and potential breach of sanctions. Next, we explore the challenges faced by financial institutions in balancing trade-based money laundering compliance and business growth.

We cap things off with an article exploring the scope of the legislation on benchmark administrators based outside of the EU and the options available for them to ensure their benchmarks can continue to be used after 1 January 2020.

We hope that you will find this edition of the FSI*Review* an interesting and insightful read.

Ho Kok Yong
Financial Services Industry Leader
Deloitte Southeast Asia

In this issue

To receive a copy of FSI*Review* or the latest updates in the financial services industry, subscribe to our mailing list at sgindustries@deloitte.com.

New tech and FinTech: Embracing the opportunity and grasping the risk

A Singapore case study

The technological evolution unfolding before us is nothing short of extraordinary. Just on cognitive capabilities alone, what took living organisms more than two billion years of evolution to attain will only take advanced technology such as artificial intelligence (AI) mere decades.

The speed of technological evolution is making a huge impact on global economies, rapidly accelerating globalisation in an increasingly digital world. This, in turn, it is reshaping the way economic agents, including financial institutions, define, operate and adapt their business models as well as their social functions. In this "global-digitisation" context, there are ample opportunities for financial institutions to harness these new technologies to improve efficiency and better service their clients. FinTechs in particular represent a chance to promote collaboration within and outside of the industry. However, increasing interdependency and hyper-connectivity introduced by new technologies are also going to generate risk at multiple levels, which will require adapted response and control.

This article looks at blockchain as an example of one of the big benefits of new technologies. It also discusses the possible risks that come with embracing these technologies, and cites Singapore as a case study on how governments can help address these risks to create a more vibrant and competitive financial services landscape.

Big benefits: The case of blockchain

An example of a new technology within the FinTech space is distributed ledger technology (DLT), also known as blockchain. This technology is expected to progressively disintermediate transactional ecosystems like trade finance, securities trading and money transfer businesses by replacing the frictions embedded within the usual transaction processes such as reconciliation, confirmation and settlement with faster, cheaper and more integrated processes.

Traditionally, the transactional ecosystem is centralised and has one single trusted part. DLT decentralises the ecosystem with trust built upon and reinforced by a number of participants. The more blocks (transactions between the participants) there are, the longer and stronger the chain (trust between the participants). Eventually, there will be more stability within the ecosystem due to the very fact that collaboration is required for blockchain to work optimally, thereby de facto shifting the paradigm of competitive advantage based on information asymmetry towards more information transparency, process integration and partnership between the DLT participants.

From a chief risk officer's (CRO) perspective, private/permissioned DLT could be a fantastic opportunity to better identify, assess and manage the risks arising from the organisation's activities. It could give access to volumes of important data and information insights that allow better anticipation and sensing of risks. Together with powerful analytics capabilities, this may drastically improve decision-making for the C-suites.

Additionally, based on the assumption that DLT will lead to more collaboration within the industry, the CRO should benefit from a more collaborative risk management ecosystem. Selected critical risk information would be shared and leveraged between institutions and some efforts would be mutualised through partnership, with a view to protect the community of interests formed by the DLT participants.

The mechanism of permissions attached to a DLT can also facilitate the audit and compliance processes and lead to significant cost reductions for financial institutions. Eventually, it should contribute to better management of the systemic risk, a priority for the regulator.

In the long term, DLT could very well pave the way for a more sustainable and inclusive economy, based on mutual trust, active collaboration and partnership of its participants for better protection of the global social ecosystem.

Consider the risk

DLT is just one example of many new FinTech that present vast opportunities to improve the business environment and make it more transparent and efficient in the long term. However, we are in very early stages of "global-digitisation" yet, and it is far too premature to know exactly what the future consequences and implications will be.

Furthermore, with every opportunity comes risks and these risks need to be addressed so that the primary purposes of deploying new technologies can be kept intact: to facilitate sound business relationships between organisations, enhance the identification and management of emerging risks, and eventually help protect the public's interests and promote a sustainable and resilient economy.

Risk #1: At the company level
Financial institutions will need to address the high level of complexity that DLT and other FinTech are progressively introducing. Failure to address this will result in opaque black boxes that no one really understands or controls. Hence, the CRO needs to be engaged as early as possible and at the strategic level to put together a robust governance and control framework that considers the implications of new technology usage in the organisation. The implications, particularly in terms of operational risk, can be significant, with the multiple impacts of digital transformation and FinTech on anti-money laundering and countering the financing of terrorism (AML/CFT), data privacy, outsourcing and cyber-risk.

Risk #2: At the industry level
There is fierce competition within the financial services industry. Incumbent players such as banks and insurance companies are potentially in danger of losing their usual intermediary and fiduciary functions to emerging FinTech companies and the highly disruptive services such as peer-to-peer financing and public/permission-less DLT. In addition, the involvement of the big technology firms (BigTech) such as GAFAM (Google, Amazon, Facebook, Apple and Microsoft) will also contribute to reshaping the financial services industry going forward. In this context of heightened competition, the financial services organisations that can offer the best experience and interface to clients and work out the best partnerships and alliances with both FinTech and BigTech will thrive. In an era of perceived regulatory divergence within the financial industry, the role of regulators will be critical to harmonise requirements and expectations across industries.

Risk #3: At the society level
The social impact made by new technologies such as Internet of Things, robotics process automation and machine learning is especially significant in the areas of privacy and employment. There have been ethical questions raised around the number of jobs that could eventually be automated and handled by computers and algorithms in place of actual people. Bill Gates recently advocated for a tax on robots in order to compensate for the replacement of the workforce. South Korea is the first country to introduce a robot tax in 2017. So far, there is no clarity on what this might mean for societal evolution in the medium term, and studies tend to diverge on whether it will create or destroy jobs in the future. But, all agree that our dependence on machines will continue to increase dramatically.

Risk #4: At the humanity level
Artificial Intelligence (AI), and the anticipated exponential learning curve some observers believe will come with it in the future, may fundamentally reshape our existence. It may even threaten it if we do not define strict rules to maintain control of these technologies and prevent the reaching of the critical inflexion point where the relation between machines and humans shifts. Computer scientist Ray Kurzweil talks about "singularity", referring to the phenomenon when machines will surpass and increasingly widen the gap between artificial and human intelligence. If we are not vigilant, there may come a time where machines will be able to use their own AI to create even more intelligent machines and supplant the human race.

How Singapore addresses these risks

In his opening remarks at the Singapore FinTech Festival last year, Monetary Authority of Singapore (MAS) Managing Director, Ravi Menon said, "Singapore is on the FinTech journey because we want to make pervasive a culture of innovation in our financial sector. [...] But FinTech must safeguard trust and confidence." This balance between innovation and confidence is indeed becoming increasingly fundamental in the light of the risks highlighted above. In this respect, Singapore is not only leading the way in terms of pure innovation potential but also when it comes to managing longer term implications. In particular, it relies on three fundamental pillars to do so.

1) Vision: Long term investment for the future

The Singapore government had announced, in its 2017 Budget, a S$2.4 billion investment over the next four years to support the future economy. This came on top of the S$4.5 billion invested the previous year into the Industry Transformation Programme, and S$1.5 billion into the National Research Fund and the National Productivity Fund. Each one of these investments constitutes a milestone in a clearly defined Smart Nation transformation roadmap. The recent 2018 Budget announcement complemented these investment efforts with enhancements by way of tax deductions for qualifying expenditure on qualifying R&D projects performed in Singapore, as well as for costs on protecting Intellectual Property (IP).

2) Education: Nurturing new talents into future leaders

The Future Economy Council (FEC) which drives Singapore's future economy transformation, is also leading some important initiatives in the talent space, such as the SkillsFuture Leadership Development Initiative (LDI). As stated on its website, the LDI "aims to develop the next generation of business leaders by helping aspiring Singaporeans to acquire leadership competencies and critical experiences". It offers specialised training programmes such as TechSkills Accelerator (TeSA) and SkillsFuture for Digital Workplace to help Singaporeans reskill and upskill to be prepared for the emerging technologies and the digital transformation of the economy. To emphasise the importance, the Finance Minister announced in this year's Budget that an additional S$145 million will be set aside for TeSA for the next 3 years. By investing massively in education, Singapore is creating the path whereby its people can better understand and master these new technologies.

3) Innovation: Aligning research and industry practice

Singapore is increasingly promoting innovation and has become a major innovation hub, not only in Asia but worldwide. This is also due to a strong alignment between public and private sectors. In particular, the Agency for Science and Technology Research (A*STAR), with collaboration initiatives such as Tech Depot (centralised platform to facilitate access to technology and digital solutions for local enterprises) and Tech Access (access to equipment and expertise for SME), has been instrumental in bridging the gap between academic research and the development of solutions for the industry. To augment these efforts, it was announced in the 2018 Budget that the National Robotics Programme will be expanded to encourage greater use of robotics, especially in construction sector.

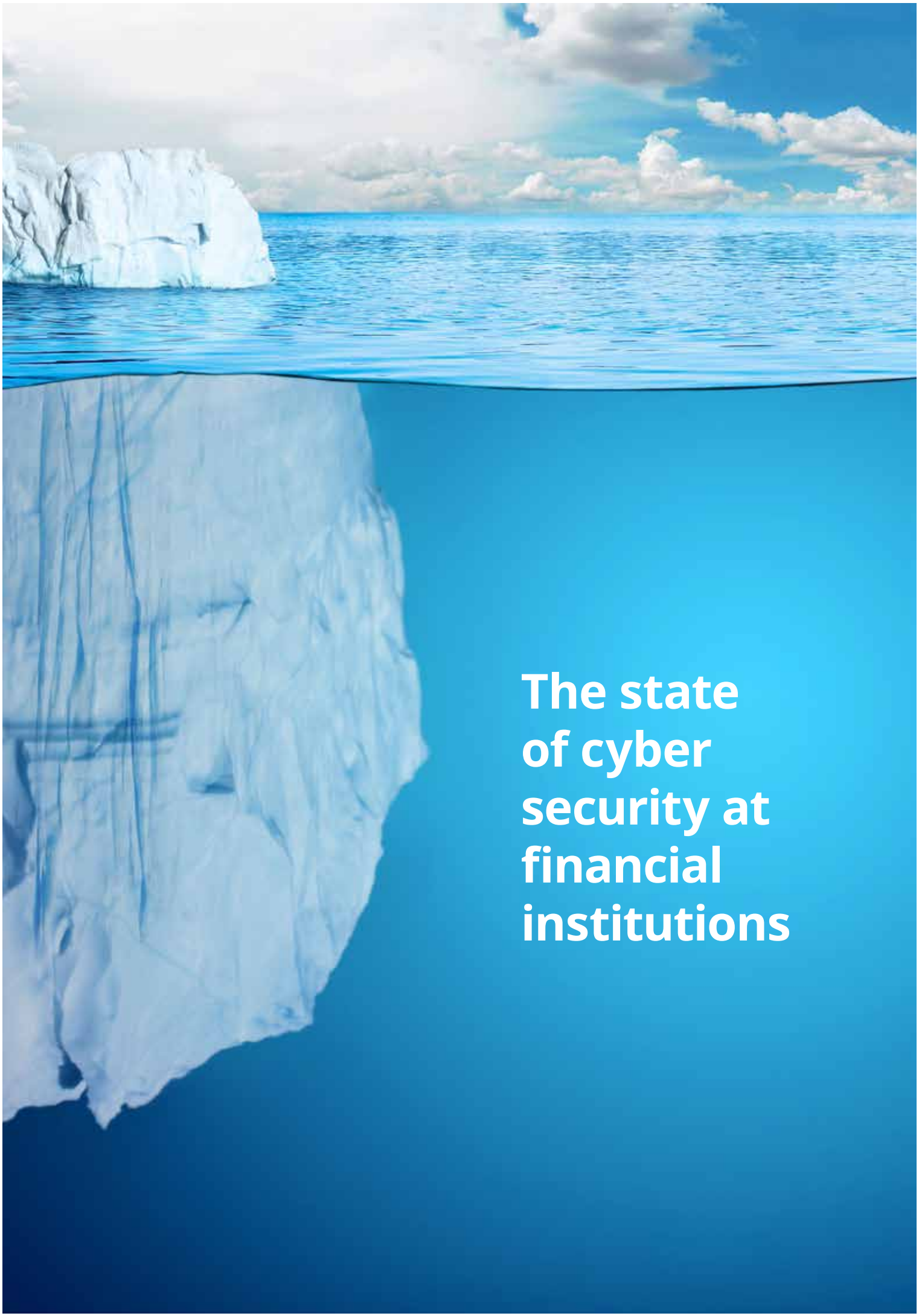
In the financial services industry, the MAS has set up a regulatory sandbox framework for the testing of FinTech innovations. This allows for more flexible rules for experimenting new products and services, while limiting the impact if something goes wrong.

Conclusion

As with any major breakthrough in human (scientific) history, the discovery, invention and use of new technologies bring about great opportunities. In the financial services industry, this could be a real game changer to the way services are provided and how the economy functions. By promoting and spreading more transparency, efficiency and collaboration among the participants, there can be better management of systemic risk, and an overall more stable, sustainable and inclusive socioeconomic environment.

That being said, in the current context of "global-digitisation", all stakeholders have to exercise caution and responsibility in the face of these new technologies. The process of innovation should not only focus on the quick wins and short-term benefits, but should also contemplate the longer term implications for the global community. In that respect, Singapore leads the way - it has defined a clear vision and plan for its future economy, is educating and nurturing today's talents into leaders of tomorrow's digital world, and is deploying significant investments for innovation while consciously aligning its public and private interests with its Smart Nation goal: "one where people are empowered by technology to lead meaningful and fulfilled lives."

This article by Frederic Bertholon-Lampiris first appeared online on the Singapore Business Review website on 13 April 2018. Frederic is an Executive Director within Deloitte Southeast Asia's Financial Services Industry practice.



The state of cyber security at financial institutions

"The increasing number of cyber attacks and its sophistication is a test of an organisation's readiness in our transforming digital world. This places a great importance on the boards and C-suites to broaden their strategy and business perspective to include security as a crucial component. The risks of not doing so is clear to everyone. It is the reason governments and regulators around the world are working closely to tackle this issue through policies and laws. However, organisations also need to take a proactive approach to build a secure, vigilant and resilient business."

– Thio Tse Gan, Cyber Risk Services Leader, Deloitte Southeast Asia

How do you measure what "good" looks like when it comes to cyber security at financial services companies?

Deloitte surveyed chief information security officers (CISOs) from 51 companies about how they are discharging their responsibilities in protecting the digital fortresses at banks, investment management firms, insurance companies, and other financial services institutions. The results provide a preliminary snapshot of how many financial institutions may go about handling cyber security, while generating intriguing insights that warrant further exploration.

Overall, we found organisations working within a broad spectrum of cyber security strategies, structures, and budget priorities. Our findings suggest that clear differences exist within the industry based on company size, maturity level, and even ownership structure.

About the survey

The survey was fielded by the Financial Services Information Sharing and Analysis Center (FS-ISAC), in conjunction with Deloitte's Cyber Risk Services practice. Fifty-one companies participated in the pilot launch of the survey, with representation from entities both large (over US$2 billion in annual revenue) and small (less than US$500 million in revenue), as well as those in between. Respondents came from all financial sectors, albeit skewed more heavily toward the US banking community.

This exploratory study looked at a number of elements in each surveyed financial institution's cyber security operation, including how it is organised and governed, who the CISO reports to, the level of board interest in the CISO's work, how much and where it externally sources risk management functions, as well as investment priorities to improve cyber security capabilities.

The survey also asked respondents to report on their cyber security maturity level, under the four-level National Institute of Standards and Technology (NIST) framework[1]. About half of respondents had their maturity level assessed by a third party, while the remainder were self-assessed. Note that the results presented in this article may not represent the full diversity of practices in the industry due to the small sample size.

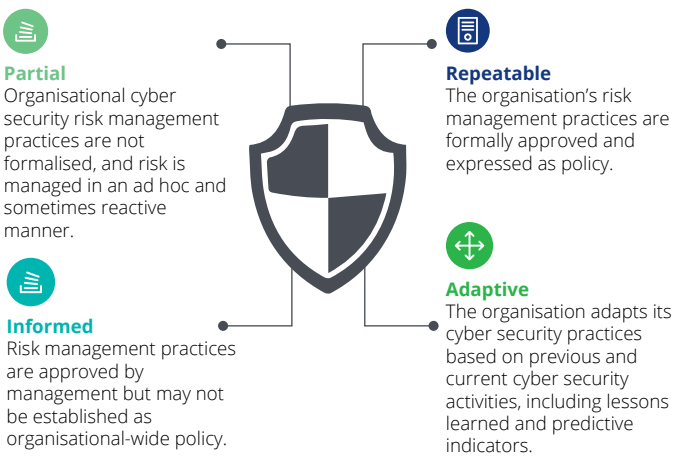
Characteristics often differ by maturity level

While it's important to have an adequate budget for cyber security, how a programme is organised and governed may be equally if not more impactful than how much is spent relative to a company's overall IT budget or revenue. Indeed, many companies with below average cyber security budget allocations managed to achieve a high programme maturity level, while some that had higher than average spending were actually less advanced. This dynamic could, in part, reflect the challenges larger, more complex global organisations often face in advancing capabilities versus their smaller counterparts.

We explore the different factors differentiating the risk management approaches and practices of adaptive respondents from their lower maturity level counterparts.

Accountability starts at the top. Almost all board and management committee members at responding companies were keenly interested in their company's overall cyber security strategy. However, those from adaptive companies suggest their boards are more likely to delve into the details of the cyber security budget, specific operational roles and responsibilities, as well as the programme's general progress than are boards of less advanced peer companies. Respondents from informed companies (Figure 1), which fall two tiers below adaptive on the maturity scale, reported their boards were typically significantly less interested in reviewing current threats, programme progress, and security testing results.

Figure 1: Cyber security maturity levels



[1] National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cyber security," Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Shared responsibilities make a difference. More than one-half to three-quarters of respondents had a fully centralised cyber security function. Respondents from adaptive companies were more likely to favour a hybrid approach: featuring centralised functions, but with each business unit and/or region given strategy and execution capabilities and coordinating with one another. Multiple lines of defines are maintained. Most respondents from adaptive firms said their organisations tended to have two separate, independent lines of cyber defines: the first involving security at front line units, and the second being organisation-wide cyber risk management operations.

Cyber risk exposure is distributed. Two-thirds of those from adaptive companies said their organisations had purchased adequate cyber insurance to cover almost all expected loss scenarios, while one-quarter had insurance to cover at least one-half of their anticipated exposure.

Outside support is sought. Respondents from companies with less mature security programmes were more likely to externally source their cyber security functions or personnel than were adaptive companies. However, across the board, the most prevalent outside source of help was with "red team" operations, in which a company tests its preparedness to be secure, vigilant, and resilient given the threat of a cyberattack.

Size tends to matter when it comes to cyber security programmes

The study raised a number of other points of distinction when it comes to how larger financial institutions responding to the survey handle their cyber security operations. Among the more noteworthy observations:

Financial services institutions may not be allocating enough resources. For the largest financial services companies, analysis of available survey data seems to suggest that their cyber risk management budgets can range anywhere from 5 percent to 20 percent of the total IT budget, with a mean of about 12 percent. In Deloitte's experience working with clients, 20 percent of IT budget is higher than what is designated at most organisations, but this could be attributable either to the method respondents used to account for total spending (capital outlay vs. annual expense) or where they are in their cyber security investment programme (some could be in a "build" phase, where initial investments are higher but level out over time).

One-half of the large financial services companies reported that cyber risk management spending was US$20 million or less. Even if one were to assume these companies invested the most and earned the least revenue within the respective ranges for those categories, this means that one-half are spending one percent or less of revenue on this area. Given the potential operational disruption, reputational damage, investigation and customer costs, and remediation expenses that could emerge from a single successful breach, this may not be enough[2].

Type of ownership makes a difference. Publicly held financial services companies responding were likely to spend more than their privately owned counterparts for cyber security. Among large public financial services companies, about one-third had a budget in the US$4 million to US$20 million range, while a slightly higher percentage budgeted more than US$100 million. This contrasts with respondents from large private financial services institutions, nearly all of whom indicated that their cyber security budgets were in the US$4-20 million category. This dynamic likely reflects concerns at public financial institutions over a potential multiplier effect from a high-profile breach, which could roil shareholders and analysts as well as undermine market capitalisation.

Meat and potatoes over dessert. Survey respondents spent more than two-thirds of their cyber security budgets on operational activities, vs. less than one-third on transformational initiatives, with cyber monitoring and operations taking up the biggest share of budget and staff allocations. By size, respondents from large companies indicated that less than one-third of their cyber risk management budgets was allocated to transformational initiatives, while those from midsize and smaller companies reported allocating only around one-quarter of budgets to transformation.

Comparisons to similar measures for IT spending overall vary, but recent research from Ovum suggests that financial services firms spend about 56 percent of total IT budgets on running the business and 44 percent on projects to change the business[3]. Although the way respondents defined "operational" vs. "transformational" may be partly responsible here, our survey sample seems to suggest that spending on cyber risk management may need to pivot to keep up with the level of spending on innovation by the business overall.

CISO reporting relationships vary. According to our survey, company size is likely to be a factor in a financial services company's cyber security reporting structure. More than one-half of CISOs responding from smaller companies reported directly to the chief executive officer, which likely reflects a flatter organisational structure. At the largest responding companies, the CISO was more likely to report to the chief information officer (CIO), chief operating officer, or chief risk officer (CRO). Half of the midsize respondents said their CISO reports to the CRO.

Innovation is a top priority. Respondents indicated there are clear priorities surrounding which cyber security capabilities are most important for investment. Respondents rated mobile, cloud, and data/analytics as the top-three priorities for adoption at their companies in the next two years, while embedding cyber defences into these new digital initiatives took top rank as the most important business issue with security implications.

When it comes to new investments, survey respondents indicated that innovation and emerging technology are top-of-mind for CISOs, with cloud, data and analytics, and social media topping the list of technology items that warrant attention at the large firms.

[2] The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. Deloitte Review 19. 25 July 2016. https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

[3] Informa, Ovum 2016 ICT Enterprise Insights Survey (Financial Services & Payments).

Where might financial services institutions go from here?

While this survey represents a small sample of the financial services community, the results nevertheless indicate steps companies can consider as they continue to upgrade their cyber security capabilities and maturity level. In many cases, these observations seem to reinforce the fact that there is a wide spectrum in the maturity of cyber risk management throughout the industry. As a whole, companies should keep raising their game to stay on top of evolving cyber exposures while enabling secure innovation.

To help improve the balance between risk and innovation, financial institutions should consider the following actions:

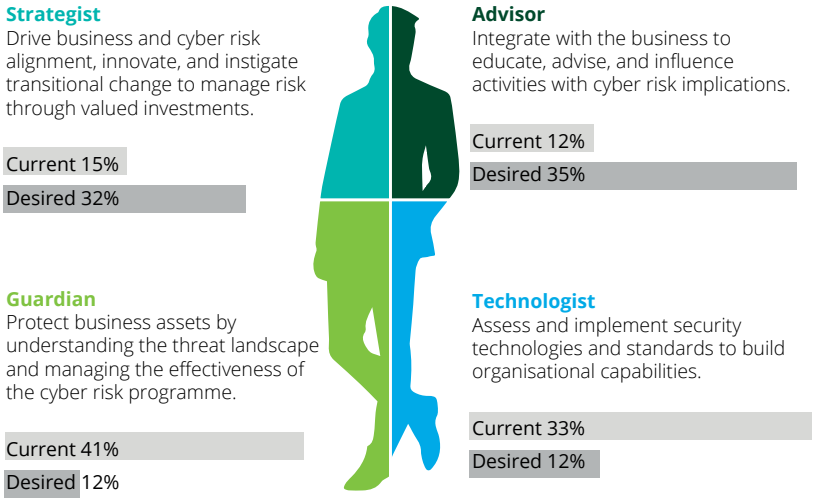
Proactively engage the board. Provide board members with the details of how management is addressing this critical exposure. Their heightened attention will likely not only keep top management more focused on perfecting their approach and improving metrics, but such high-level scrutiny should also resonate throughout the organisation.

Engage the entire organisation in cyber security. With so few full-time employees devoted to cyber security, everyone in the organisation should understand and embrace their vital role and responsibilities in detecting intrusions, reporting red flags, and maintaining good security hygiene to help prevent events from happening in the first place and limit the damage if they do occur.

Provide multiple lines of defence. Companies should aim to embed cyber security practices and personnel within business units and regional offices to support the central cyber risk management team. As it should be everyone's job to manage cyber risk, make sure awareness and duties permeate the organisation, and share accountability.

Alter the mix of a CISO's responsibilities. Last but not least, to do their jobs effectively, CISOs should be reporting beyond the CIO and regularly interact outside the IT department. Most CISOs already wear a number of hats, but unfortunately many are often focused on their traditional roles as technologists and guardians. Deloitte's work with CISOs suggests that they spend almost 74 percent of their time in these more tactical roles. As the job has become more complex, however, they should strive to spend two-thirds of their time as strategists and advisors (Figure 2) to better support their management teams and boards[5].

Figure 2: The four faces of the CISO



Getting to the next level on cyber security

As cyber security is expected to continue to be an integral function for financial institutions, improving capabilities will likely be an ongoing challenge as threats keep evolving in scope, technique, and sophistication. Financial services institutions should keep adapting to stay one step ahead of threat actors that intend to do them harm.

At present, we have just scratched the surface when it comes to cyber security benchmarking. Future surveys are likely to seek more information on cyber security budgets and headcounts by maturity level and company size to create benchmarks such as:

- Maturity score by NIST domain
- Cyber security spending as a percentage of IT spending, as well as per FTE
- Number of cyber risk FTEs as a percentage of information security and total IT personnel

However, while benchmarks could help financial institutions assess their readiness to handle cyber risk, remaining secure, vigilant, and resilient also likely requires the industry to look beyond their own experiences and continue working together with broader communities facing the same threats.

As efforts by FS-ISAC demonstrate, collaboration on cyber security is important across the financial services industry and within individual industry sectors. At a minimum, financial institutions should closely follow cyber war stories to learn from the experience of peers. This could help financial services institutions avoid having to reinvent the wheel in efforts to protect their people and systems against the latest cyber threats.

This article is an excerpt of the report, "The state of cyber security at financial institutions" published in May 2018 by the Deloitte Center for Financial Services. To receive a copy of the full report, drop us an email at sgindustries@deloitte.com.

[4] The new CISO: Leading the strategic security organization. Deloitte Review 19. 25 July 2016. https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

[5] Deloitte Cyber Risk Services CISO Transition Lab analysis, Deloitte Financial Advisory Services LLP.

Trade-based money laundering compliance: A balancing act

Over the years, regulators and standard setting agencies categorised trade finance as a "higher risk" business for money laundering, terrorist financing and potential breach of sanctions. Growing complexities and volumes of trade flows create opportunities for criminal organisations to launder proceeds of crime through the international trade system.

Financial institutions have difficulty in monitoring and implementing controls in their trade finance business to combat trade-based money laundering (TBML). The problem is exacerbated by lack of clarity in the compliance requirements and regulatory expectations in many jurisdictions.

Whilst controls can be put in place for documentary trade, greater issue lies in open account situations where the financial institutions have far less visibility on the underlying transaction.

In documentary trades (regardless of the letter of credit meeting international and legal standards) where there are TBML and economic sanctions issues, it may still warrant an action from the financial institution to report or otherwise take necessary steps to protect itself. This requires the delicate balancing act of "not tipping-off" customers.

In this article, we highlight some key challenges in balancing TBML compliance and business growth, including those provided in the International Chamber of Commerce (ICC), the Bankers Association for Finance and Trade (BAFT) and Wolfsberg Paper on TBML and our experience working with the industry. Deloitte believes that these challenges resonate with financial institutions given the operational difficulties they encounter. This also follows the release of the industry paper, "Best practices for countering trade-based money laundering"[6] on 14 May 2018 by Singapore's Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP).

What is the global regulatory standard?

Over the last few years, international standards-setters such as the Financial Action Task Force (FATF) and industry groups such as BAFT, ICC, Wolfsberg Group and the Hong Kong Banking Association (HKAB) have provided thought leadership and guidance on international standards or best practices in combatting TBML.

These groups outline best practices and local regulators enforce these guidelines by imposing legally binding requirements on individual financial institutions. Key regulators that have set the tone on regulatory expectations for financial crime compliance, including TBML are the Monetary Authority of Singapore (MAS) and Financial Conduct Authority (FCA) in the U.K.

Arguably, the MAS has set the highest standard and should financial institutions implement their controls based on these standards, it is a safe assumption that such financial institutions would have satisfied expectations of all regulators they are subject to via their global footprint. Having said that, this remains a good and educated guess. Accordingly, there could be more done by regulators globally to also set their expectation and clarify their position on TBML compliance standards in their jurisdictions.

While, there are a number of references available on best practices and regulatory expectations for TBML, financial institutions face the challenge of operationalising and implementing these requirements and/or best practices. In addition, the global footprint of these businesses bring with it the challenge of harmonising compliance standards across borders.

Key challenges

Getting the price right

Financial institutions should assess the reasonableness of the price of goods quoted when facilitating trade transactions. The issue faced by the industry is the lack of reliable and publicly available statistics and data on prices of myriad of goods, except for commodities. Added complexity in price assessment arises when goods traded are spare parts and constituents or otherwise components of larger (and potentially specialised) items.

An international agreement on the level of diligence needed by financial institutions for "price checks" will help. This should be based on a defined risk-based approach of a financial institution. For example, under the following conditions, an intrusive price check may not be necessary:

- The customer is a well-known and reputable business
- The customer has a long standing relationship with the bank
- The price variation of the goods is within an acceptable range (based on standards developed based on the bank's own data on transactions)
- There are no alarming anomalies noted

Banks should also establish their own internal database for price guidance based on the transactions handled. According to ICC, BAFT and Wolfsberg, a greater level of transparency can be achieved if governments, regulators or enforcement agencies and trade bodies partner with financial institutions to share information and establish a single, consolidated pool of commodity prices.

[6] Best practices for countering trade-based money laundering. The Association of Banks in Singapore. May 2018. https://abs.org.sg/docs/library/best-practices-for-countering-trade-based-money-laundering.pdf

Know the goods transacted

Specialist knowledge is often required to determine whether the goods involved in transactions have dual-use. Dual-use goods include software, technology, documents and diagrams which can be used for both civil and military applications. The goods can range from raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. They could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers. Unfortunately, financial institutions typically have limited knowledge to ascertain this.

It is common that trade documents do not provide a detailed description of the goods or components of the same. A good practice to identify dual-use goods in trade finance transactions is to screen goods, preferably using a paid database, to ascertain its status. Armed with the financial institution's profile and knowledge of the customer gathered at the onset on the goods intended to be traded, details of the transactions conducted by the customer and parties involved, length of the relationship and the issues seen during the life-cycle of the customer, staff can identify red flags which suggest that dual-use goods may be supplied for illicit purposes. In this matter, financial institutions may need to take a heightened risk approach.

Import/export licensing

Financial institutions are not always in a position to determine if an export licence is required for a trade transaction. The counterparties to a trade transaction are in a better position to determine that an export licence is required and obtain such licence if it is required.

Financial institutions should obtain advice on the typical goods that require such licences in key jurisdictions that they have exposure to via their customers and transactions, and seek their customers' confirmation that where required, such license has indeed been obtained.

Detecting duplicate letters of credit, bills of lading and invoices

How will a financial institution know if a customer is submitting duplicate or fraudulent trade documents? Unfortunately, financial institutions don't have access to information of other financial institutions. Hence, their view on a transaction and its documentation is limited. The best practice is to check with the issuing bank when a financial institution is presented with trade documents, verify the original documents and check for any obvious anomalies in the documentation over and above screening the parties involved. Relying on a MT700 message[7] alone may not suffice. If multiple banks are seeking confirmation from the issuing bank, it should trigger a red-flag review on the part of the issuing bank who can alert the other banks and take necessary action.

Circumvented yet again?

Regardless of the checks conducted and controls put in place by financial institutions, it is difficult to confirm that a customer is involved in circumvention. When a trade ends at a port of discharge on paper which is further confirmed by end of the vessel route, it is quite an art to ascertain that the goods were transported later to a sanctioned or a high risk jurisdiction or party or otherwise routed to a jurisdiction where there are restrictions placed on certain goods. The potential use of tug boats and feeder vessels in such a situation add complexity to ascertain circumvention. The use of these tug boats and feeder vessels blurs the ability to track the vessel's route as well.

Financial institutions can only make best efforts to make enquiries to confirm that there is no suspicion of circumvention in a case where a customer trade ends at a port or jurisdiction known (based on experience) for circumvention, neighbouring a sanctioned or high risk country or a country where certain goods are restricted or where there is suspicion of transhipment without a good reason. In some ports and jurisdictions, given their international trading hub status, transhipment by known customers may be normal.

Still stuck in paper-based trade finance?

Despite the level of technology available, trade finance processes continue to be largely paper-based. This reduces financial institutions' efficiency and effectiveness in implementing risk management controls. Continued need for manual input and review or monitoring of trade transactions is a tedious task prone to human error. Financial institutions with large trade books suffer from costly and time-intensive manual review of paper documents.

While there is a lack of a holistic view of the information flows in trade transactions and seamless capability to spot red-flags in a systematic manner, we believe that the developments below that need to be urgently addressed will make a positive impact in TBML compliance:

- Digitisation of trade documents to reduce human error and expedite the process while decreasing the costs of manual trade documents and transactions review;
- Technological developments to fully automate trade transactions and implement pattern based recognition systems (which if at all may only be attainable to larger financial institutions) or a fully automated trade solution that tracks the transaction which performs screening, checks on vessel routes, and assesses red-flags from data on the customer, documentation, transaction, shipment and payment, until the transaction is completed with human intervention, analysis and judgment as required; and

[7] According to SWIFT, MT 700 is a message sent by the issuing bank to the advising bank. It is used to indicate the terms and conditionals of a documentary credit which has been originated by the Sender (issuing bank). Link: https://www.swift.com/node/21326

- A blockchain solution across the industry to create a sustainable ecosystem for all parties to a trade transaction as a utility that tracks a transaction based on digitised uniquely identifiable trade documents (we are hopeful that this materialises) and bills of lading.

Financial institutions may also consider implementing Optical Character Recognition (OCR) capabilities in the trade finance process, which makes scanned text computer-readable so that relevant information can be extracted and stored in electronic form and analytic tools be applied to analyse the data for anomalies, red-flags and trends. Though this may not solve the issue in its entirety, it nevertheless is a good start to build a broader digital solution in a modular fashion.

What's next?

With the growth in the volumes of international trade and given the complexity in the trade finance business, improving TBML compliance measures and controls require a collaborative effort between relevant agencies and financial institutions. To summarise, global and inter-agency cooperation is needed with the industry to:

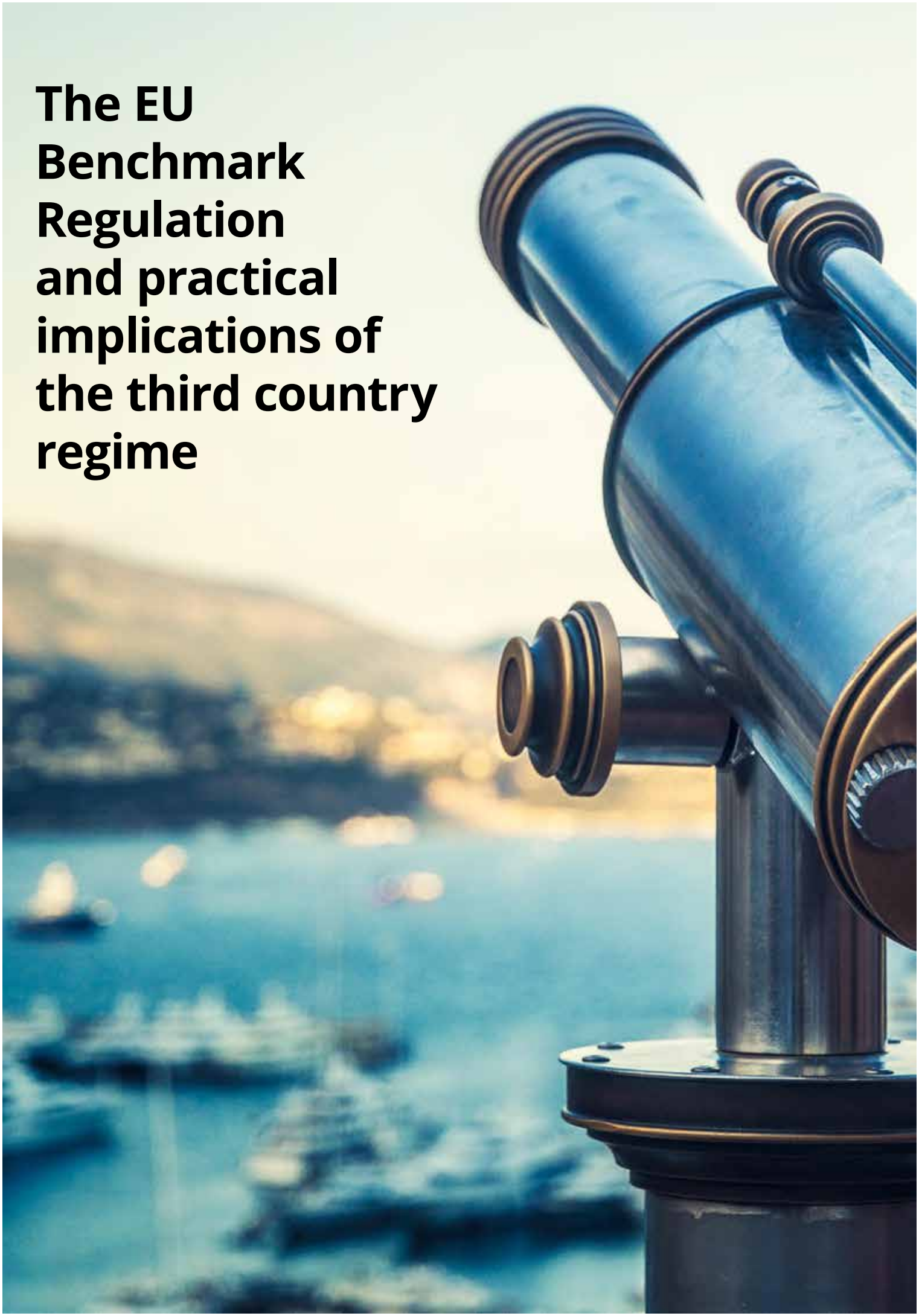
- Create global trade data for price-checking purposes.
- Agree on the reasonable standards for due-diligence required on the part of the financial institution with regard to dual-used goods. Practically, unless it is an outright red-flag or a weapon of mass destruction, it is quite difficult to determine whether some items are going to be used for dual or wrongful purposes. For example, certain chemicals or chemical content of goods such as fertilizer, cannot always be concluded as being intended for dual use by a customer whose business is to manufacture chemicals or fertilizers or otherwise by a customer who has an established need or use of these in their customary business.
- Lobby a policy shift where rules should equally apply on importers and exporters:
  - Pre-registration with customs authorities before these parties can conduct international trade. In addition, customs authorities could mandate unique identifiers for goods imported and exported and pre-certification on dual-use goods and restricted or embargoed goods before the use of any banking facilities as well as monitor tug boats feeder vessels use;
  - Importers and exporters should conduct Know-Your-Customer (KYC) and Customer Due Diligence (CDD) checks on their clients;
  - Shipping companies should check on the buyers and sellers, goods being transported and ensuring that International Maritime Organization (IMO) numbers are provided on the bill of lading; and
  - Insurers to conduct CDD on the parties at the same standards that FIs do for trade transaction purposes.
- Custom authorities can mandate the provision of the Harmonised System (HS) Classification of Goods and International Maritime Dangerous Goods Code (IMDG) to assist banks in screening goods or assessing red-flags related to goods.
- Agree on a global set of TBML regulatory standards which are harmonised across all jurisdictions to create clarity and a level playing field for banks regardless of its location and size of business.
- Establish a Trade Transparency Unit which enables global partnership to leverage trade data as well as import/export data from other participating countries to effectively analyse trade information.
- Streamline procedures to help detection of duplicate bill of lading where shipping companies could potentially "centrally" register a bill they have issued which can be checked by the bank for authenticity.

Given the complexity of trade transactions (and transactions monitoring globally), regulators and enforcement agencies could support an initiative to conceptualise an industry-wide surveillance system where a bank should be able to holistically view or visualise a trade transaction and parties involved in the same. This can sharpen the ability of the bank to conduct transactions monitoring or surveillance and detect red flags based on available data.

A paradigm shift in the manner in which surveillance is undertaken has to change to become cutting-edge with greater public private partnership and, ultimately, creation of an eco-system for global view of trade transactions.

This article is written by Radish Singh, SEA Financial Crime Compliance Lead for the Deloitte APAC Financial Crime Network.

The EU Benchmark Regulation and practical implications of the third country regime



The EU Benchmark Regulation (EU BMR) became effective on 1 January 2018 and whilst the transitional provisions mean that many of the requirements are not fully effective until 1 January 2020, benchmark administrators – particularly those based outside of the European Union (EU) – should already be taking action to ensure preparedness for that date.

In this article, we explore the scope of the legislation on benchmark administrators based outside of the EU and the options available for them to ensure their benchmarks can continue to be used in the EU after 1 January 2020.

What is a third country administrator?

Any benchmark administrator based outside of the EU that provides benchmarks or indices that are used in the EU by a supervised entity will be subject to the third country regime requirements of EU BMR and thus defined as a third country administrator. Subject to the transitional requirements discussed further below, for the benchmarks administered by a third country administrator to continue to be used in the EU after 1 January 2020, the third country administrator must comply with the requirements of EU BMR.

Options for third country administrators

The legislation provides third country administrators with three options to comply with the requirements and continue to administer their benchmarks for use by EU supervised entity post 1 January 2020. In choosing which option is suitable, third country administrators should consider a number of factors including the benchmark's current and potential future presence in the EU, the number of benchmarks in scope as well as the complexity of administering the benchmarks.

Equivalence

Consistent with Equivalence regimes set out under other pieces of EU legislation, EU BMR provides that the competent authority (i.e. the local relevant financial markets regulator) of the third country should adopt legislation or rules equivalent to EU BMR in their local jurisdictions and then seek approval from the EU for Equivalence.

The Equivalence option is dependent on third country competent authorities electing to seek Equivalence with the EU. Given that we are a number of months into the transitional period, we would encourage engagement between third country administrators and their competent authority as soon as possible to discuss whether Equivalence will be sought.

Where Equivalence is granted, the scope of any new rules or legislation implemented in the third country will be dependent on ESMA's assessment of the third country's current legal framework and supervisory practice; for example, depending on whether ESMA determines that the third country's legal and supervisory framework is equivalent to the requirements set out in EU BMR or, at least equivalent to, the requirements of the IOSCO principles. Whatever the requirements, it is likely that third country administrators would need to apply for authorisation from their local third country competent authority.

Additionally, third country competent authorities may choose to limit the Equivalence regime to specific benchmarks and/or administrators. Therefore, if a third country benchmark administrator is not included in the scope of the Equivalence regime then they will need to select one of the two alternative options discussed further below (i.e. Recognition or Endorsement).

Recognition

Recognition requires an administrator located in a third country to have legal representation in the EU through which the regulatory oversight is affected by an EU competent authority. The EU legal representative will be required to carry out oversight responsibilities and will effectively be accountable for the provision of the third country benchmarks within the EU.

The location of the EU legal representative will be dependent on the third country administrator's presence in the EU or where their existing third country benchmarks are being used in the EU. The regulation sets out a waterfall of requirements on Article 32(4) that assists third country administrators to determine the location of the EU legal representative.

As part of the Recognition application, the EU legal representative is required to evidence the third country administrator's compliance with the IOSCO principles to the relevant EU competent authority. This can be achieved either by engaging an external independent assurance provider to carry out an independent assessment or by a certification provided by the relevant third country competent authority.

Endorsement

In order to seek Endorsement, third country administrators will need to engage an authorised EU benchmark administrator. The authorised benchmark administrator will then apply to its local competent authority for Endorsement of the third country administrator's benchmarks (for example, this could be achieved through a commercial arrangement with the EU benchmark administrator providing this service).

The EU benchmark administrator must demonstrate that it will have a well-defined role within the accountability framework of the third country administrator and that it will supervise the administration of the endorsed third country benchmarks on an on-going basis.

The EU administrator will also need to prove to its competent authority that it has the necessary capabilities to monitor the provision of the third country benchmarks. Note, however, the regulation stipulates that the endorsing administrator needs to provide an explanation of the objective reason for the provision of the endorsed benchmark in a third country and for it to be endorsed in the EU.

Timeline and transitional arrangements

The Q&A from ESMA issued on 8 November 2017 provided further clarity on third country transitional arrangements under EU BMR which differ from the transitional arrangements for EU countries. Figure 3 below highlights that third country benchmarks are able to be used in the EU throughout the duration of the transitional period to 31 December 2019.

Additionally, third country benchmarks that existed prior to 1 January 2020 can continue to be used in existing contracts post 1 January 2020 until maturity, without the need for administrator complying with EU BMR.

However, the use of existing benchmarks provided by third country administrators in new contracts created after 1 January 2020 is not permitted, where the third country administrator has not complied with the third country requirements of the Regulation. Additionally, the use of benchmarks created by a third country administrator post 1 January 2020 is not permitted, unless the benchmark is in compliant with the third country requirements Regulation.

Figure 3: A summary of the timeline and transitional arrangements under EU BMR

<table>
<tr><th></th><th>Pre-2020</th><th></th><th>Post-2020</th></tr>
<tr><td rowspan="2">Existing</td><td rowspan="2">Existing third country benchmarks are allowed to be used in the EU</td><td>Use in existing contracts</td><td>Use in new contracts</td></tr>
<tr><td>Third country benchmarks are not required to be authorised</td><td>Third country benchmarks are required to be authorised</td></tr>
<tr><td>New</td><td>New third country benchmarks are allowed to be used in the EU</td><td colspan="2">Third country benchmarks are required to be authorised to administer new third country benchmarks to be used in the EU</td></tr>
</table>

Next steps

We set out below a series of considerations for third country administrators:

Consider if you want to continue to provide third country benchmarks in the EU

Third country administrators should assess how widely and to what extent their benchmarks are currently used within the EU, as this will help them to evaluate whether EU BMR compliance is necessary from a commercial perspective. Compliance may entail significant cost, which may not be justifiable. Administrators may determine that a better course of action would be to limit the use of their benchmarks to non-EU supervised entities after the necessary deadlines per above. Should they wish to continue to provide benchmarks to EU supervised entities beyond the relevant timelines, third country administrators should consider the following next steps.

Establish whether an Equivalence regime will be come into effect

Third country administrators should seek to establish with their local competent authority whether there are any current plans to seek Equivalence with ESMA.

If there are plans for Equivalence, third country administrators may need to comply with new rules or requirements, for example the IOSCO principles or, possibly, the requirements of the EU BMR which third country competent authorities may enforce locally. Third country administrators will need to be prepared as the changes could be significant.

Evaluate whether Recognition or Endorsement is a better option

If no Equivalence regime is being sought, third country administrators will need to decide between the two remaining options: ***Recognition*** or ***Endorsement***.

Recognition: There will be cost implications in setting up an EU legal representative. The significance of these costs will depend on whether the third country administrator is a subsidiary or part of a group which also comprises EU supervised entities.

Notwithstanding, third country administrators will need to consider how much work is needed to make to align their overall governance and control framework to the IOSCO principles and across geographies. Furthermore, firms would need to factor in the costs and benefits involved in obtaining independent assurance from an independent external auditor.

The proposed changes to various EU regulations by the European Commission published on 20 September 2017 could add a layer of complexity to the decision making. Currently the regulation requires third country administrators, together with their EU legal representative, to apply to the relevant local EU competent authority to seek authorisation for Recognition. However, the proposed changes to ESMA's powers could mean that third country administrators, together with their EU legal representative, apply directly to ESMA instead. These proposals need to be agreed by the European Council and Parliament in negotiations and the entire process of finalising the rules can take 18 months or more. Firms should monitor any developments but at the current time follow existing requirements for seeking Recognition.

Endorsement: This will mean partnering with an authorised EU benchmark administrator that would likely be external to the company; firms must consider the suitability of this business relationship. Cost and operational considerations need to be assessed, as the endorsing company needs to be embedded within the firm's governance framework and have a well-defined role in the accountability framework. These need to be assessed against the strategic objectives of the company as well as regulatory efficiencies that Endorsement could bring to third party administrators. This suitability assessment will also depend on the quantum and complexity of benchmarks being endorsed.

Prepare for sustained IOSCO compliance

The Third Country Regime defined under the EU BMR clearly indicates that as a minimum, third country administrators should comply with the IOSCO principles for whichever option has been selected. Hence, we would encourage third country administrators to appropriately align their governance, risk and control framework for their benchmarks administration operations to the IOSCO principles.

Conclusion

Third country administrators should be considering the costs and benefits of each of the options under the Third Country Regime. As we near the deadline for transitional arrangement, firms will need to decide on next steps, and start to implement their plans, engaging with industry and regional forums throughout the transitional period and formulate communication strategies to their clients and the markets in which they operate.

This article is written by Dave Roberts and Foo Chuan Jian. Dave is Executive Director and Chuan is a Senior Manager; both are a part of Deloitte Southeast Asia's Financial Services Industry practice.

SEA Financial Services Practice

Southeast Asia Financial Services Leader

Ho Kok Yong
kho@deloitte.com
+65 6216 3260

Business Leaders

Audit & Assurance
Tay Boon Suan
bstay@deloitte.com
+65 6216 3218

Consulting
Kevin O'Reilly
kevinjoreilly@deloitte.com
+65 6800 1038

Financial Advisory
Jeff Pirie
jpirie@deloitte.com
+65 6216 3168

Financial Advisory
Radish Singh
radishsingh@deloitte.com
+65 6530 8077

Risk Advisory
Somkrit Krishnamra
somkrishnamra@deloitte.com
+66 2034 0000

Tax & Legal
Michael Velten
mvelten@deloitte.com
+65 6531 5039

Country Leaders

Guam
Tung Wei-Li
wtung@deloitte.com
+1 671 646 3884

Indonesia
Rosita Sinaga
rsinaga@deloitte.com
+62 21 2992 3100

Malaysia
Anthony Tai
yktai@deloitte.com
+60 3 7610 8853

Philippines
Bonifacio Lumacang
blumacang@deloitte.com
+63 2 581 9000

Singapore
Ho Kok Yong
kho@deloitte.com
+65 6216 3260

Thailand
Somkrit Krishnamra
somkrishnamra@deloitte.com
+66 2034 0000

Vietnam
Thinh Pham
thpham@deloitte.com
+84 839100751

Deloitte.

Singapore FinTech Festival 2018
Connect. Engage. Collaborate.

The world's largest platform for the global FinTech community is back and Deloitte is proud to once again support the Singapore FinTech Festival as a Grand Sponsor.

Join us from 12 to 16 November as the movers and shakers of the global financial community gather in Singapore for a week-long celebration of FinTech. This year's Festival promises to be bigger, better and jammed packed with even more exciting activities!

Through a series of distinct events, the Festival provides a platform for stakeholders to connect, engage and collaborate, sparking new ideas for the future.

Visit www.deloitte.com/sg/fintechfestival2018 for more information.