THE PAN ASIAN REGULATORY SUMMIT 2018

PRE-EVENT REPORT

the answer company™
THOMSON REUTERS®

Against the backdrop of increasingly complex regulatory regimes and the regulators' continued focus on individual accountability and stringent enforcement action, 2018 has been a challenging year for financial institutions across Asia. With a combination of exclusive regulatory announcements and industry case studies, the 9th annual Pan Asian Regulatory Summit will discuss the latest regulatory developments and challenges impacting financial markets in the region.

From fintech and regtech innovations to the latest data and conduct regulations, this report presents the key themes for this year's summit through a series of articles published on Reuters News and the Thomson Reuters Regulatory Intelligence platform.

For more details and to register for the event, please visit:

http://financial-risk-solutions.thomsonreuters.info/panasianregulatorysummit2018

Contents

Regulatory inconsistency in Asia-Pacific adds 10 percent to business costs

Niall Coburn, Senior Regulatory Intelligence Expert, Thomson Reuters

An inconsistent approach to the regulations of investment products, capital markets, banking and asset management in the Asia-Pacific region has reduced cross-border investment, an official said. It has added between 5 and 10 percent to the cost of doing business according to Nick Malyshev, head of regulatory policy at the Organisation for Economic Cooperation and Development (OECD) .

Research carried out by the OECD indicates that foreign direct investment (FDI) can increase by as much as 15 percent where countries choose to harmonise laws and regulations.

WHAT IS REGULATORY DIVERGENCE AND WHY IS IT IMPORTANT FOR COSTS?

Regulatory divergence is the degree of inconsistency that arises between different jurisdictions from the implementation of regulations. Inconsistencies from one country to another can make it difficult to understand the application of the law and even lead to different enforcement outcomes.

This in turn adds to the costs of doing business in the region; financial institutions find that they need larger compliance departments to deal with the plethora of regulations and/or need to pay for legal advice on the intricacies of doing business in another jurisdiction. It can be hard for smaller firms to bear such costs.

"The complexity of regulatory procedures can have a negative impact on FDI. If countries that have complex regulatory procedures move toward the average of the top half of best performers, [i.e., countries who simplify regulations], FDI could increase by about 15 percent, according to some, but not all specifications," the OECD said in a report published in 2015.

"Regulatory divergence, in the Asean region alone, adds approximately $800 million to the costs of doing business in the financial sector," Malyshev said.

The need for banks and firms to deal with hundreds of small differences in regulation, ranging from data privacy to securities laws, also added confusion, he said.

WHAT CAN BE DONE?

There are a number of positive moves afoot in the region, such as harmonisation of cross-border collective investment schemes and the implementation of the stock connect between Hong Kong and China. Governments and regulators still need to work harder to bring about regulatory harmonisation, however, and there are a number of strategies which they might consider:

- ***Adopting international standards***
Rather than introducing separate regulatory regimes, countries should consider adopting international standards. For example, the recent drive to bring in management accountability has led to the introduction of five different approaches, in the UK, Hong Kong, Singapore, Malaysia and Australia. All the regimes set out to achieve the same outcome, which is to make senior managers accountable for operational business decisions, yet global firms will need to know how to deal with each one in their jurisdictions, adding to the cost of doing business.

- ***Businesses can lobby regulators for harmony***
Businesses need to lobby regulators in the region to push for harmony where there is a clear business case to do so. For example, on January 25, 2018, the EU implemented the General Data Protection Regulation (GDPR) to improve the privacy protection afforded to EU citizens and their personal data. The regulation took many years to draft and there was extensive consultation with industry. Asia-Pacific firms that are dealing with EU citizens must consider not only their own data protection legislation but also the GDPR. Indeed, given the comprehensive nature of the GDPR, many international banks are adopting this legislation as best practice. Asia-Pacific countries might consider following suit, rather than having numerous data protection laws in each jurisdiction.

- ***Greater involvement of financial institutions***
Financial institutions could be more involved in the way standards are developed throughout the region, emphasising the need for a consistent approach and assisting cross-border cooperation.

BENEFITS FOR DEVELOPING ECONOMIES

The negative effect of regulatory divergence on foreign direct investment is sizeable, and both regulators and financial institutions need to think more carefully about harmonisation in a world where many financial products are marketed internationally. This could also have major benefits for developing economies in the Asia-Pacific region such as Cambodia, Vietnam and Indonesia.

Hong Kong regulator says its approach to regulation showing results

Trond Vagen, Asia Editor, Thomson Reuters

The increasing focus given to corporate misconduct in recent years has had a big impact on market behaviour in Hong Kong, said the city's top regulator. Ashley Alder, chief executive of the Securities and Futures Commission (SFC), said the regulator had intervened early in several serious cases of market misconduct in order to "safeguard the interests of investors and suppress illegal, dishonourable and improper market practices".

The regulator on Wednesday published a newsletter highlighting some of the more serious cases it had intervened in in the past year, making use of its powers under the Securities and Futures (Stock Market Listing) Rules (SMLR) to protect investors.

The cases highlighted in the regulator's newsletter highlight both issues before and after initial public offerings, including concerns about information provided to investors, high concentrations of shareholdings and dilutive share offerings. In several cases the regulator has used the SMLR to object to listings due to concerns over the company's compliance with the listing rules.

Corporate misconduct has been singled out by the SFC in recent years as one of its major focus areas, with the enforcement division setting up a special task force to investigate cases where investors may have been deceived by dishonest market practices. The regulator has also adopted a "front-loaded" style of regulation, where it seeks to intervene in potential cases of market misconduct at an early stage.

Regulators have also voiced concerns over cases where a whole range of market participants, such as brokers, sponsors and companies applying to be listed, have acted together to deceive the market.

"Many of you would have read about or heard of networks of companies which use cross holdings of assets and shares to try to create higher valuations for the listed companies within the network," said Brian Ho, the SFC's executive director of corporate finance, in a speech given last week. "Undeniably, there are companies or persons who engage in misbehaviour at the expense of public shareholders. This can only have a negative impact on the reputation of our market."

Noting that enforcement could only take place after misconduct has happened and losses have been incurred, in a process that could take a long time, Ho said the front-loaded approach was an important tool to help change market behaviour.

He said the regulator and the stock exchange had acted to reduce volatility on the Growth Enterprises Market (GEM) in recent years through the issue of guidance to sponsors and underwriters on what standards of conduct the regulator expected. He also said concerns over capital raising exercises had led to the exchange introducing a ban on highly dilutive rights issues and open offers.

"The typical patterns of problematic behaviour can be seen in transactions involving securities issuance, such as deeply discounted fund raisings, share consolidations and subdivisions," he said. "These transactions materially dilute the voting rights and value of public shareholders' investments, and some result in a transfer of value to the new subscribers."

Ho also said the regulator had advanced its use of the front-loaded approach from post-IPO cases to pre-IPO listing application cases, in particular using its powers under sections 6 and 8 of the SMLR to object to a listing or suspend trading. He said the regulator had used its SMLR powers in such cases around 40 times in 2017, compared to only two or three cases per year in the past.

"Issuers, sponsors and other parties involved in an IPO process can be investigated at the application stage where we have grounds to suspect that the SMLR provisions are triggered," he said. "There will be enforcement consequences if breaches of the Securities and Futures Ordinance (SFO) are identified, irrespective of whether the listing application is withdrawn."

Hong Kong's MIC regime has made big difference, says regulator

Trond Vagen, Asia Editor, Thomson Reuters

Hong Kong's Manager-in-Charge (MIC) regime, introduced in July last year by the Securities and Futures Commission (SFC), has given the regulator a more structured view of firms' management and accountability, said Julia Leung, deputy chief executive.

It has also been well-received in the market, with compliance officers reporting it had made a welcome difference in fulfilling their roles, said Leung, who is also head of intermediaries.

Leung told the SFC Regulatory Forum in Hong Kong earlier this month that the Manager-in-Charge regime had improved firms' governance structures and ensured that the right people were set to look after important business lines.

"We have seen boards filled with people who are MICs, and their job responsibilities, particularly for global organisations with local subsidiaries, are very clearly delineated," she said. "Some of them actually have put [together] operating committees and filled them with MICs so that they can make better decisions."

Another important benefit of the regime was that it had helped drive behavioural changes at firms, Leung said.

"When you are designated as an MIC you are suddenly much more aware of your responsibilities and [the] accountability that comes with that," she said.

She said the SFC had come upon the idea of implementing an MIC regime as part of an attempt to address problem issues it had identified in firms' governance. She said the SFC's licensing department had not been receiving structured management information, such as details of which managers were in charge of key business lines.

While the SFC has had a "responsible officer" regime in place under the Securities and Futures Ordinance (SFO), she said a common problem the regulator encountered was that the people appointed as responsible officers were typically not those "calling the shots".

Some firms also had boards populated by directors without any real responsibility, she said.

Leung said that although, in the past, the regulator could have used the liability provisions in the disciplinary chapter of the SFO to chase down wrongdoers. a typical problem was that the lack of structured management information meant it was difficult to pinpoint who may have been in charge at the time of a regulatory breach that may have happened years ago.

The implementation of the MIC regime had definitely enhanced the governance structure, she said.

"We also have much better alignment of senior management with responsible officers," she said.

SIMPLE BUT EFFECTIVE

Andrew Procter, partner at Herbert Smith Freehills and a former senior regulator, said in comparison with other regulators which have introduced similar regimes — the UK Financial Conduct Authority with its Senior Managers and Certification Regime and the Australian Securities and Investments Commission (ASIC) with its Banking Executive Accountability Regime (BEAR) — the SFC's model was both simple and effective.

"[The SFC] did a very nice job of introducing the changes with a minimum of complexity but covering a wide range of firms," he said. "The UK [regulator] produced literally thousands of pages of consultations. There are already four versions of the senior managers regime, and they've not yet rolled it out to the 50,000 non-banking firms. [Leung] produced 23 PowerPoint slides, and one of them said 'any questions?' It was a model of how things can move in Hong Kong regulation."

While the scheme implementation had been successful, Procter said that firms, whether in Hong Kong, Australia or the UK, did not appreciate going through the change process, although they had come out on the other side with better systems in place.

"They have to be dragged from where they are to where they need to get," he said.

"What [Leung] did to cover the field was a very simple requirement around the alternative to what in the UK are the responsibility maps and in Australia the accountability maps," he said.

"There's not as much prescription in either of those two jurisdictions, but they are the key documents that force people to think of 'how things are really done around here'. What [Leung] has done is calibrate a very simple one-line requirement for complexity in firms. Now, she's going to hold them accountable for that."

He also advised regulators to give firms some space to settle into the new regimes, whether in the UK, Australia or Hong Kong.

"If it is true that it is not an enforcement-led program, and that it is about doing things better and about prevention, then the senior managers, or the managers-in-charge, or the accountable managers in Australia, will need to be given space to do the things that are expected of them," Procter said.

"And when something goes wrong, for them not to immediately be dragged to enforcement. There has to be more space for a supervisory dialogue between senior management and the regulator."

Chu Gang, chief operating officer of China International Capital Corporation (CICC), said there was a trend of introducing regulation to ensure financial institutions were run to higher standards.

In that sense, he said, the SFC's Manager in Charge regime was right for the Hong Kong market, particularly given the large influx of Mainland Chinese firms setting up in the territory in recent years.

"Hong Kong's mix of intermediaries has been changing: you have global firms which have strong connections to their home country regulators, very complex businesses and matrix reporting formats, and strong culture and all that," he said.

"Then, you have local firms, where the business model tends to be simpler and small, and now additionally a large number of mainland firms coming into the market. They are in varying stages of development, both in terms of business complexity and also [regulatory] experience."

Some 13 percent of licensed corporations in Hong Kong are controlled by Mainland Chinese corporates, according to figures released by the SFC last year. The SFC has in the past expressed concern that some mainland firms circumvent the licensing process by acquiring dormant businesses that are already licensed by the SFC, complete with responsible officers in place, to evade scrutiny and the responsibilities of being a licensed person, while still gaining entry to the Hong Kong market.

MAS proposes individual accountability regime for senior managers

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

The Monetary Authority of Singapore's (MAS) recent proposals to strengthen individual accountability of senior managers and raise standards of conduct in financial institutions were inevitable following similar moves in the UK, Hong Kong and Australia.

The consultation paper, launched on April 26, set out MAS' expectations on boards and senior managers with respect to individual conduct and behaviour. The proposed guidelines apply to all financial institutions including banks, asset managers, securities firms and financial advisers.

MAS said the proposed guidelines are not intended to be prescriptive and it is the responsibility of financial institutions to hold their senior managers accountable for their actions and ensure proper conduct among their employees.

"Clear accountability and proper conduct are important elements of good governance and sound business practice. Persistent misconduct and a lack of individual accountability by persons in charge will erode public confidence in our [financial institutions]. We expect the boards and senior management of [financial institutions] to instil a strong culture of responsibility and ethical conduct," said Ong Chong Tee, MAS' deputy managing director (financial supervision).

MAS TOOK WAIT-AND-SEE APPROACH

Following Hong Kong's implementation of the Manager-in-Charge regime last year, there was speculation about whether Singapore would follow suit. MAS had been taking a wait-and-see approach to see how similar regimes in other jurisdictions would work out, including what problems would arise and how those regimes were implemented, said Joanna Pearson, partner at Simmons & Simmons JWS in Singapore.

"Singapore operates as a key financial centre and many financial institutions based here would have already been subject to similar regimes in other jurisdictions. Many of them would have given thought to the Manager-in-Charge regime in Hong Kong and the Senior Managers and Certification Regime [SMR] in the UK. They will have gone through the identification of senior managers' responsibilities in other jurisdictions," she said.

FORMALISED RESPONSIBILITY MAPPING

Breaches and misconduct had arisen in the past whereby senior managers at financial institutions were not entirely clear who should be responsible for those problems and who should be taking action. MAS' guidelines seek to require financial institutions to go through the process of identifying responsible persons in a systematic way, Pearson said.

She pointed out that the word "individual' is of great significance since it requires one person to be responsible for an area within financial institutions.

"Effectively it is about identifying individuals who are responsible and identifying any gaps. One of the objectives of the guidelines is to ensure that a thorough process is undertaken and documented, that the individuals know that they have that responsibility and understand what that means in practice and what is expected of them," she said.

Some financial institutions have, on a more informal basis, carried out responsibility mapping.

"This [set of] guidelines is to formalise that. What it does not require is notification of the identified persons. Instead, compliance will be assessed via the MAS's ongoing supervisory process. MAS has not included a requirement to report who each of the key responsible persons are, which is very different to the UK regime which requires financial institutions to prepare a very detailed responsibilities map. There is greater notification under the UK regime," Pearson said.

MAS' GUIDELINES MORE FLEXIBLE

While MAS' proposed guidelines have largely followed UK's SMR and Hong Kong's Manager-in-Charge regime, its proposals are less prescriptive, Pearson said.

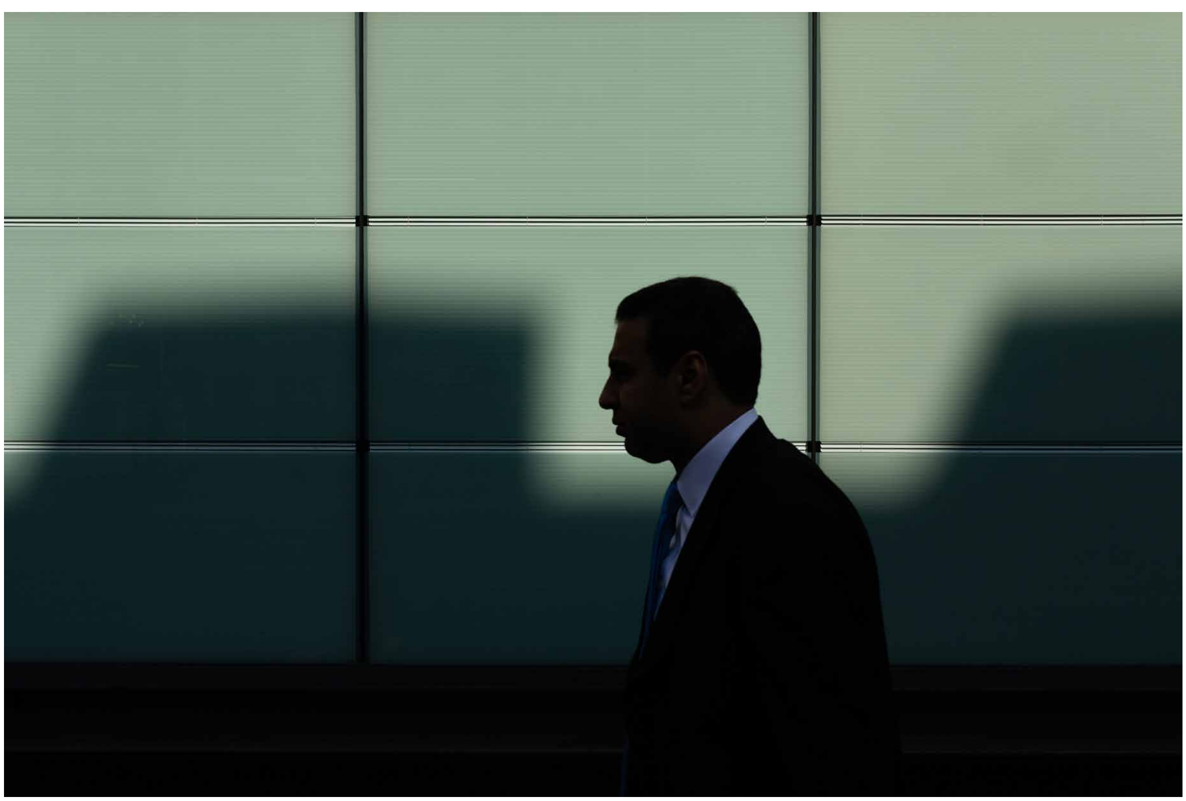
"I haven't yet done a line-by-line comparison, but broadly it is fair to say MAS' guidelines are a little more flexible. They set out a set of desired outcomes and guidelines but they do offer financial institutions some flexibility [in] how they are implemented. The regimes elsewhere are more prescriptive," she said.

One of the challenges presented by the individual accountability regime is the complication that financial institutions are likely to face when they have to identify responsible individuals for branches and locally-incorporated entities, Pearson said.

"Having a prescriptive regime may not work well," she said.

OBJECTIVES AND FIVE OUTCOMES

MAS' proposed guidelines seek to reinforce financial institutions' responsibilities in three main areas: by increasing the individual accountability of senior managers; by strengthening the oversight of employees in material risk functions, and by reinforcing standards of proper conduct among all employees. To achieve these



objectives, MAS has set out five accountability and conduct outcomes which financial institutions are expected to work toward.

In outcome 1, senior managers who have responsibility for the management and conduct of functions that are core to the financial institutions' operations are clearly identified.

In outcome 2, senior managers are fit and proper for their roles, and are held responsible for the actions of their staff and the conduct of the business under their purview.

In outcome 3, financial institutions' governance framework is supportive of, and conducive to, senior managers' performance of their roles and responsibilities. Financial institutions' overall management structure and reporting relationships are clear and transparent.

In outcome 4, employees in material risk functions are fit and proper for their roles, and subject to effective risk governance as well as the appropriate standards of conduct and incentive structure.

Finally, in outcome 5, financial institutions have a framework that promotes and sustains the desired conduct among all employees.

CONDUCT AND CULTURE

Nizam Ismail, head of financial services at RHTLaw Taylor Wessing in Singapore, said the consultation paper clearly articulated that MAS is focusing on not just the hardware in financial institutions such as systems and compliance process, but also the software aspects such as culture and management oversight.

"It is not enough just having a set of compliance processes; you need to have a robust culture, and management has to set the tone at the top. It puts a lot of scrutiny on financial institutions to demonstrate that they have processes in place to measure culture and conduct of good behaviour," he said.

MAS' approach to conduct and culture, summarised in three aspects — namely, promote and cultivate, monitor and assess, enforce and deter — is also striking, Nizam said. "Promote and cultivate" is about promoting a culture of trust and ethics at financial institutions through engagement with the industry. "Monitor and assess" is about monitoring the culture and conduct at financial institutions, and "enforce and deter" talks about MAS' approach to breaches and misconduct which will involve enforcement, investigation and prosecution.

"It is MAS' nuanced approach that says, 'We will work with you to ensure everything is ok, but if you misbehave, we will go after you'", he said.

Nizam pointed to the first outcome in the guidelines which, he said, was significant. Senior managers at financial institutions are subject to MAS rules as long as they have oversight responsibility or decision-making authority, even if they are outside of Singapore.

"I see this as creating incentives for financial institutions to ensure most of critical decision-making functions reside in Singapore," he said.

Outcome two, which requires senior managers to have responsibility for staff and for the conduct of the business under their purview, has raised the question of whether the senior manager should be held responsible if a member of staff misbehaves.

"That will be quite an interesting area. It goes into whether the staff [member]'s misconduct is something which could have been prevented by the manager or whether it is because of compliance framework that is not sufficiently robust," Nizam said.

Financial institutions are also required to have in place a governance framework that is supportive of senior managers' roles and responsibilities, and to ensure that the overall reporting structure is clear and transparent, as set out in the third outcome, Nizam said.

In the fourth outcome, employees in material risk functions are required to be fit and proper in their roles because such roles have an impact on the financial institutions' risk profile, according to Nizam.

"There are a couple of expectations. Board and senior management should identify ... these persons who are in material risk functions and make sure they are fit and proper on an ongoing basis. This includes matters like setting decision-making authority, risk limits, and supervisory oversight," he said.

People in material risk functions are also subject to a few requirements including continuous training and an appropriate incentive structure that is aligned with their role and the risk they take.

"Financial institutions have to look at the risk outcome before they decide how much they want to pay the person for performing the function. The intention is to make sure the manager who performs the function is suitable for the role. They are expected to perform," Nizam said.

The fifth outcome, which requires financial institutions to implement a framework that promotes and sustains the desired conduct of all employees, is a formalised whistle-blowing channel, according to Nizam.

"MAS expects a whistle-blowing function, a framework that escalates misbehaviour. More broadly, the new framework does create an expectation for financial institutions to think of setting up systems to measure good compliance culture and conduct," he said.

Implementation challenges expected for MAS's proposed individual accountability regime

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

The Monetary Authority of Singapore's (MAS) recent proposed guidelines on individual accountability of senior managers, while flexible in its approach, has also seen questions being raised in a number of areas.

MAS' guidelines are one of the main aspects of its efforts in fostering a culture of ethical behaviour and responsible risk-taking in the financial services industry. The guidelines seek to reinforce financial institutions' responsibilities in three main areas: individual accountability of senior managers; oversight of employees in material risk functions; and standards of proper conduct among all employees.

Five accountability and conduct outcomes which financial institutions are expected to work toward were also proposed: identifying senior managers who are responsible for the management and conduct of functions critical to financial institutions' operations; holding senior managers responsible for the actions of their staff and the conduct of the business under purview; having a governance framework that is supportive of senior managers' performance of their roles and responsibilities; subjecting employees in material risk functions to effective risk governance and appropriate standards of conduct and incentive structures; and putting in place a framework that promotes and sustains the desired conduct among all employees.

IMPLEMENTATION DETAILS NOT ADDRESSED IN CONSULTATION PAPER

Yvette Cheak, founder of ACE Compliance Pte Ltd in Singapore, said the consultation paper was well-drafted and covered important issues such as cross-border concerns, areas where there may be regulatory differences and who makes the decision when something happens.

While the consultation paper largely set out broad principles, some of the details have yet to be ironed out, Cheak said.

"When it comes to the implementation, you need to be very clear about where the responsibility lies and who is accountable. For example, some foreign banks are locally incorporated in Singapore but they have holding companies overseas. Should the local regulation come first or the regulation from their home country? Also, for banks operating in Hong Kong and the UK, the level of accountability may not be the same in the two jurisdictions," she said.

Cheak also pointed out the potential challenges that some foreign banks which operate as branches in Singapore, such as those from Spain, France, Malaysia, Thailand and Indonesia, may encounter.

"How should these banks approach this if they operate as a branch? Who is going to be responsible? Who gives the direction? Who is accountable? Where is the accountability? The consultation paper hasn't specifically gone to the extent of addressing this branch versus subsidiary issue," she said.

MAS recognises that there are financial institutions operating in Singapore which have head offices overseas, and it has acknowledged that it may not always be appropriate to have an employee in Singapore who is accountable for decisions that were made overseas, said Joanna Pearson, partner at Simmons & Simmons JWS. This means that financial institutions may not have all their managers in Singapore.

"It will be interesting to see how this plays out. Financial institutions will identify the relevant functions and key persons in Singapore who will be classified as senior managers. There are differences in this respect in terms of the type of institutions, depending on how they are structured, whether they are locally incorporated or operate as branches," she said.

Identifying senior managers is important to MAS because financial institutions are structured differently, Pearson said. This explains why MAS deliberately offers flexibility by setting out desired outcomes rather than prescriptive requirements, she added.

"What would need to happen when this regime comes in is that individual institutions would need to look at their own arrangements and structure in order to identify the senior managers and other individuals in material risk functions," she said.

HOLDING SENIOR MANAGERS RESPONSIBLE FOR THE ACTIONS OF THEIR STAFF

Questions have also been raised about the proposed third outcome, which holds senior managers responsible for the actions of their staff and the conduct of the business under purview. Nizam Ismail, head of financial services at RHTLaw Taylor Wessing in Singapore, said consideration would need to be given to a few aspects including whether, when an employee misbehaves, it is completely something that could have been prevented by the managers or whether it is due to compliance lapses or the lack of a robust framework. He cited corruption involving a staff member as an example.

"If the manager has knowledge of the employee carrying out the act, then he can be taken to task. But if the company has [a] good policy but the employee ignored it, you need to treat it differently," he said.

CONDUCTING DUE DILIGENCE ON EMPLOYEES

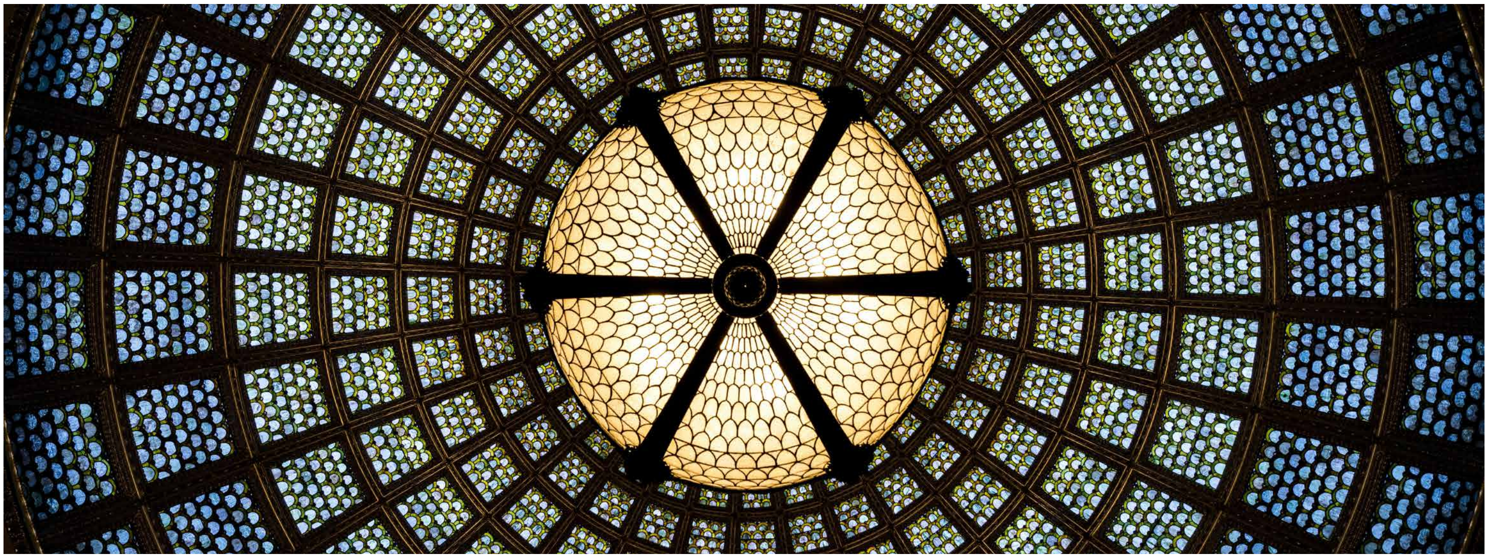
Another potential challenge for financial institutions is MAS' requirement to carry out due diligence on employees, especially those who are in material risk functions. This requirement may put financial institutions in a dilemma, Cheak said.

"Financial institutions need to consider whether their employees are fit and proper, and that would require them to carry out due diligence of employees. Does it mean that financial institutions have to do due diligence on existing staff?" she said.

NOT MANDATORY BUT EXPECTED TO COMPLY

While MAS' proposed guidelines are not mandatory, financial institutions operating in the city-state are expected to comply, Cheak said.

"Financial institutions will have to take some self-governance to comply with these guidelines. It is a good risk management practice in terms of responsibility; it is also about protecting your institutions and your systems. Financial institutions are all linked in one way or another," she said.



HKMA actively seeks to make Hong Kong the booking centre of Asia

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

The Hong Kong Monetary Authority (HKMA) is actively promoting the special administrative region as the Asian booking centre for international banks and is in talks with market players individually to address their concerns.

The idea of making Hong Kong or Singapore the Asian booking centre first began two years ago among international market participants involved in over-the-counter (OTC) derivatives, amid concerns about Brexit.

While Hong Kong and Singapore have shown willingness to become large booking centres of Asia, regulators in the two jurisdictions have their concerns, particularly in relation to recovery and resolution, said Simon Topping, regulatory partner at KPMG China who is based in Hong Kong. Asian regulators are concerned about how Asian accounts which are booked overseas will be treated in the event of a resolution, he said.

"It's a complicated issue for both home and host regulators. The HKMA has been asking global financial institutions why equities are booked in London when Hong Kong is in fact the logical place to book them. HKMA is going through case-by-case to understand why banks find it difficult to book their business here," he said.

HKMA REDUCING IMPEDIMENTS

HKMA received a number of comments from financial institutions about issues such as large exposure, funding and taxation, which are the main challenges for global banks wanting to book their business in Hong Kong. The HKMA's market development team is actively looking at how to position Hong Kong as the booking centre, including the need to make changes to the law, taxation, and expediting the process for model approval, particularly for market risk model, according to Topping. "HKMA is working on these issues to reduce the impediments to banks booking in Hong Kong. If banks book their business in Asia, especially if they want to build a large amount of derivatives business, the main issue is the market risk model. The standardised approach for market risk will provide a high capital charge. Any bank with a large amount of market risk needs to be on a market risk model approach in order to reduce the capital charge," he said.

PUSH AND PULL FACTORS

With increasing concerns about the aftermath of Brexit, and following the implementation of the Markets in Financial Instruments Directive II (MiFID II) in January this year, more global financial institutions have begun to take an interest in the idea, according to Keith Pogson, senior partner at EY in Hong Kong.

"These factors act as a catalyst for many European and American banks to start reconsidering which booking model and booking hub they will use in Asia, and for what purpose," he said.

There have also been other push and pull factors. With London being one of the world's major booking centres, the UK regulators have been concerned, privately, about the impact of Brexit on booking of business and risk management accountability, although publicly they have always maintained that London remains open for business, and some financial institutions have seen this as a push factor, according to Pogson.

There are several pull factors. For example, Asian clients tend to prefer to have their transactions booked in Asia, an indication to foreign financial institutions to book such trades in the region. Nor are financial institutions operating in some jurisdictions particularly pleased at the prospect of continually having to fulfil regulatory requirements from overseas regulators. Some international banks have looked upon these as pull factors to consider Hong Kong or Singapore as the potential booking hub, Pogson said.

"There was a perceived competitive disadvantage for the foreign banks versus the local banks and so people are looking at this, and a lot of thoughts are going into making somewhere in Asia the booking hub with a new booking model," he said.

MAIN CHALLENGE: CAPITAL EFFICIENCY; APPROVAL PROCESS FOR MODEL VALIDATION

But challenges abound. Regulatory capital issues have emerged as a top concern, particularly regarding model approval, which will in turn determine the amount of capital banks are required to hold, according to Pogson. Most banks which have been booking their business into the UK, by far the major booking centre, generally have model approvals and various forms of models that give them an advantage in meeting capital requirements and the corresponding amount of capital they are required to hold.

Regulators in Hong Kong and Singapore, however, have historically been slower to approve models, and that has posed the biggest uncertainty to banks, Pogson said.

The HKMA market development team has spent much time attempting to understand the concerns of players including business environment considerations such as tax and training of people, as well as industry-specific concerns such as whether Hong Kong has an approval process in place for model validation.

"Without the model approval, banks are faced with using the standardized model and that will result in dramatically higher capital. Some foreign banks have less of an issue because they have [capital] buffers in Hong Kong but once these are exhausted, it will be expensive for them. Capital efficiency is the number one issue," Pogson said.

THE FUTURE OF HONG KONG

Of the two jurisdictions, the HKMA has been more active in courting players and putting in place measures to make Hong Kong the booking centre of Asia, whereas the Monetary Authority of Singapore (MAS), while open to one-on-one conversation with banks, has been more reserved in its desire to promote Singapore as the booking centre of Asia, Pogson said.

"At the government level, Hong Kong has recognised the need to think about what will become of Hong Kong's future role as a financial centre. Financial services is by far its largest industry. If Hong Kong needs to have a sustainable future, it needs to make sure that it is the number one financial hub in the region. Singapore, on the other hand, has many initiatives in terms of its ongoing prosperity," he said.

RISK; SIZE OF BALANCE SHEET

The fact that Hong Kong, being part of mainland China, has a bigger balance sheet for taking risk unlike Singapore which is a nation state on its own, makes a huge difference, Pogson said.

"Hong Kong is able to be more aggressive in this space because it has a large balance sheet. Hong Kong's historic financial services industry is more global whereas Singapore has a smaller balance sheet and its legacy financial services industry is dominated by local players," he said.

But Pogson also pointed out that both the HKMA and MAS do not have a large appetite for risks that do not have an Asian nexus.

"Nobody is particularly interested in non-Asian risk. For foreign players, the Asian booking centre will be predominantly for Asian risks," he said.

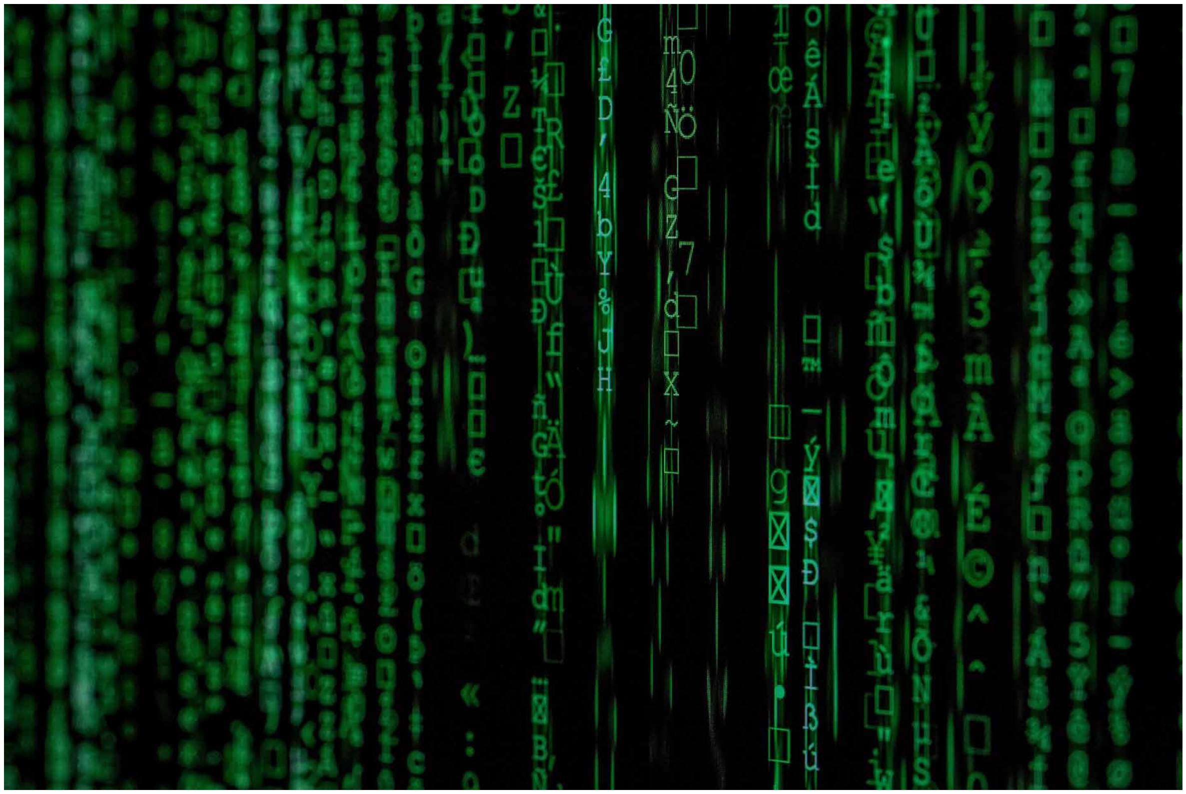
Addressing the concerns of foreign banks is not the only reason to make Hong Kong the booking centre of Asia; it is also about enticing mainland Chinese banks and persuading them to make Hong Kong their international business hub.

"For the Chinese banks, it might be slightly different. Hong Kong may be their offshore booking centre," Pogson said.

EXPLORATION

It is unlikely Asian regulators will have a one-size-fits-all policy on making their jurisdiction the booking centre because of the case-by-case nature of the portfolio and products of banks, and the set-up of the risk models, according to Pogson. While no definitive policy is in place, be it in Hong Kong or Singapore, international financial institutions are exploring both jurisdictions as the potential booking centre of Asia.

"It's a very complex area in which the regulators are reserving their judgment. I wouldn't be surprised if it is a case-by-case situation. It isn't about a change in regulation as the rules have been in place historically. It's about how favourably these are being received and the skills that are brought to bear. It's about applications from interested players and the focus of the regulators," Pogson said.



Risk data aggregation and reporting regulation triggers wider concerns about data

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

The Basel Committee on Banking Supervision's (BCBS) effective risk data aggregation and risk reporting regulation has triggered regulators' concerns about the quality of data, and they are putting more pressure on banks, a consultant said.

Also known as BCBS 239, which was introduced on January 1, 2016, the effective risk data aggregation and risk reporting regulation is targeted only at global systemically important banks (G-SIBs), and in some jurisdictions, domestic systemically important banks (D-SIBs). Even then, BCBS 239 is widely considered to cover only a small subset of the global financial services sector.

A Basel Committee report which tracks the progress of banks' implementation of BCBS 239, showed that progress has been slow so far, said Simon Topping, regulatory partner at KPMG China based in Hong Kong.

"BCBS 239 is really about making risk data more useful. It is to make the data into [a] useable and useful form. If you go back to the origin of BCBS 239, it was due to regulators having a lot of trouble getting the data they need to understand threats in the industry and any issues about banks," he said.

BCBS 239 TRIGGERS MORE DIALOGUE ON DATA

As the work on BCBS 239 progresses, regulators are beginning to ask more questions about data. They are also putting a lot more pressure on financial institutions, and in some cases, more requirements on data as a result of the whole conversation on BCBS 239, said Kevin Nixon, managing director at Nixon Global Advisory in Sydney.

"BCBS 239 has become everybody's conversation," he said.

As BCBS 239 has triggered a bigger dialogue on data, regulators now have higher expectations on a number of areas, according to Nixon. These include the quality of the systems at financial institutions that capture data and the data that comes out of those systems, and the way data gets reported internally and to regulators.

Against this backdrop, regulators are also concerned about issues that are related to data including cyber security, privacy, new initiatives such as open banking and new technology such as Cloud.

MAPPING OUT THE MOVING PIECES

Many financial institutions are now putting considerable focus on data, and that requires them to map out all the moving pieces regarding data, from regulations to new technology, Nixon said. The big challenge to any financial institution is where they want to be in the future in the face of changing regulation, technology and landscape, which will in turn determine the areas into which they want to put the most effort, he said.

"What are regulators demanding around infrastructure, privacy, cyber security and open banking, just to name a few? What does technology like the Cloud mean for storing and managing data and privacy concern? Who are going to be users of data in the future and what could it be used for?" he said.

HOLISTIC APPROACH

As banks scramble to comply with BCBS 239, much focus has been put on building an infrastructure capable of capturing data in an accurate manner. But many banks have also lost sight of future needs, Nixon said.

"BCBS 239 requires banks to capture data in an efficient and accurate manner. It is too easy to focus only on the infrastructure. To build your systems to meet BCBS 239, you need to look at not just the current needs but also what are the likely ways you are going to need to use the data. There could be two concerns: infrastructure and analytics. But you can't do one without the other. You need to look at this holistically," he said.

INFRASTRUCTURE AND DATA ANALYTICS

Data analytics, according to Nixon, is inextricably linked to infrastructure because the type of data, the amount of data required and the accuracy of data are all related to infrastructure.

"In order to do data analytics well, you need to know that the data is good. That means your infrastructure must be capable of analysing the data. You can have the best data systems in the world, but if you don't know what to do with it, you are wasting your time. You have to put infrastructure and data analytics together to make a difference," he said.

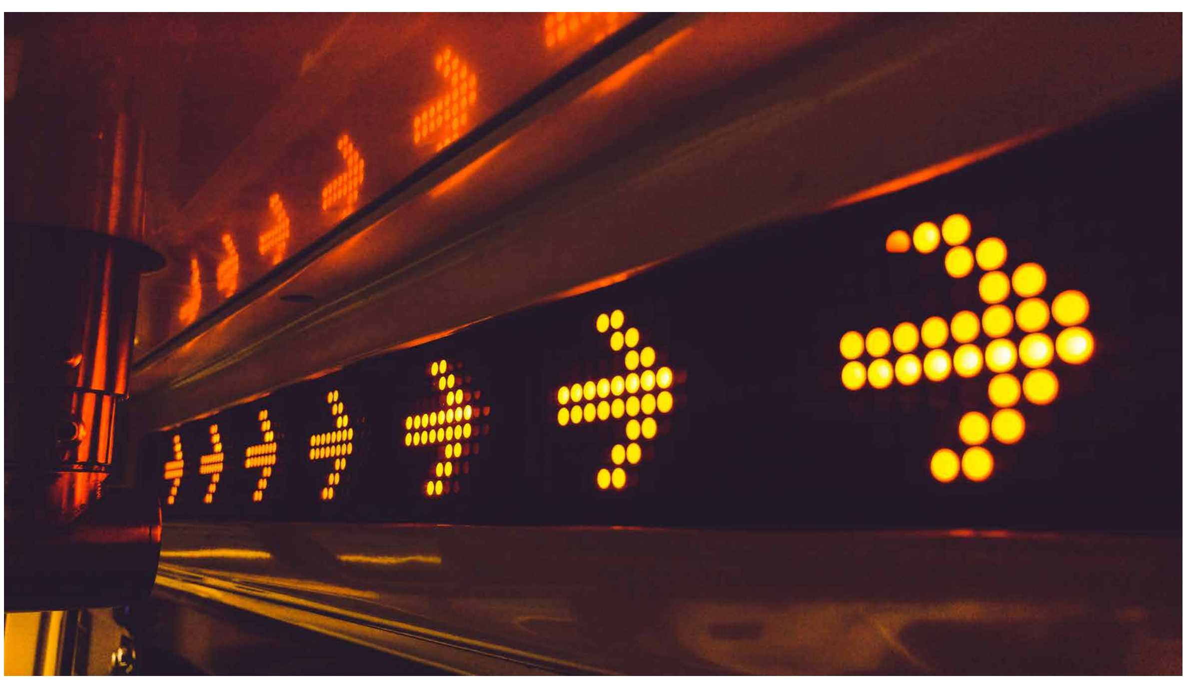
DATA PRIVACY, CYBER SECURITY AND OPEN BANKING

The proliferation of data privacy laws throughout the world, and in particular the General Data Protection Regulation (GDPR), has led to greater awareness on the legitimate and appropriate use of data.

Aside from issues such as the purpose of using the data and whether data can be legitimately used, cyber security, new initiatives such as open banking and management information systems are some of the areas that would also need to be considered, Nixon said.

Management information systems, in particular, are often neglected, as the more topical issues such as data privacy and cyber security take centre stage.

"What gets reported to the management is a big area but often overlooked. If you are not getting the good data and information communicated to you, you are not managing the company well. Business decisions are often made based on information," he said.



Regulators, financial institutions, fintech players address "a balance of responsibilities" issue in data use

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

The wider use of new technology such as cloud and blockchain by financial institutions in Singapore, and regulators' new initiatives such as open banking, have raised questions about ways to protect data.

According to the EY risk management survey 2017, 86 percent of the financial institutions surveyed have identified data as an area of emerging risk, while 80 percent viewed industry disruption due to the use of technology as the second top emerging risk.

Regulators, financial institutions and financial technology (fintech) players are beginning to weigh up "a balance of responsibilities" in the uses of data for banking services, particularly when the users sometimes involve application programming interface (API) users and third-party service providers. The issue arose largely because of concerns about potential data leakage which could result in a breach of data privacy law, as well as the threat of cyber attacks.

While MAS encourages financial institutions to adopt new technology, they have to use it within MAS' framework, said Gary Chia, head of financial services regulatory and compliance at KPMG Singapore. MAS has its expectations on financial institutions, requiring them to ensure that customer data is stored in a secured environment, he said.

"For a start, banks are subject to the banking secrecy provisions in the Banking Act. There are very clear guidelines on safeguarding of customer information. Banks are permitted to use service providers, however, these service providers will similarly need to meet client confidentiality requirements," he said.

GUIDELINES ON OUTSOURCING AND TECHNOLOGY RISK MANAGEMENT

Financial institutions using services such as cloud offered by third-party service providers are required to meet basic requirements, namely the MAS' "Guidelines on Outsourcing" and the "Technology Risk Management Guidelines", both of which state that financial institutions must require their service providers to comply, Chia said.

This means service providers must have, among other things, a disaster recovery plan and a business contingency plan in place, as well as back-up plans for systems to be up-and-running again.

"MAS' supervisory approach has not changed. A financial institution using a cloud service provider has to ensure that it first assesses the third-party service provider and that the latter meets some of the basic requirements required by MAS. Given that MAS does not have purview over service providers, the onus is on financial institutions to ensure third-party service providers follow the requirements that are expected of them," he said.

With cyber hackers on the prowl, cyber security standards for clouds must also be in place, Chia said.

According to Chris Lim, advisory partner at EY in Singapore, banks are exploring the use of cloud for storing personal data. This requires them to recognise the risk involved, which includes being aware of data sensitivity and how to achieve a balance between using new technology and data protection, he said.

MAS' VIEWS ON CLOUD

MAS' stance toward the use of cloud computing by financial institution is largely supportive. It recognises the benefits that cloud computing offers, including scalable storage solutions which allow financial institutions to meet the real-time demands of trading and analytics processes, and its scalability and resilience which give financial institutions the confidence to move their core banking systems into the cloud.

In his recent speech at the Symposium on Asian Banking and Finance held in San Francisco, Ravi Menon, MAS' managing director, pointed out that cloud computing has enhanced risk management significantly, which allows risk assessments to be "more comprehensive, more granular and more real-time".

Menon also highlighted new risks which cloud computing brings, particularly the outsourcing risks associated with cloud service providers which, he said, are much larger because of the massive amount of financial institutions' data sitting on the cloud and their reliance on cloud service providers for processing functions.

"Financial institutions have less knowledge, let alone control, of where their data are stored in a cloud computing infrastructure spanning several different jurisdictions. Data breach or loss might occur due to a natural disaster, targeted attack, or poor security processes at the CSPs [cloud service providers]," Menon said.

Outsourcing risk is further exacerbated by concentration risk, as is evident from the fact that the world's top four cloud service providers collectively had an 80 percent market share last year. About 25 percent of the core banking systems of global systemically important banks (GSIBs) now resides on the cloud, according to Menon. A large cloud service provider may, in some way, be carrying systemic risk if many financial institutions rely on it and in the event that it fails, he said.

The MAS and the UK Financial Conduct Authority were among the first regulators in the world to issue regulations or guidance on the management of outsourcing risks pertaining to cloud, Menon said.

BLOCKCHAIN TECHNOLOGY

The use of the blockchain — also known as distributed ledger technology (DLT) — in Singapore has been explored on several fronts. Three areas where the application of distributed ledger technology is used to the biggest advantage are compliance, trade finance and cross-border payments, according to Menon.

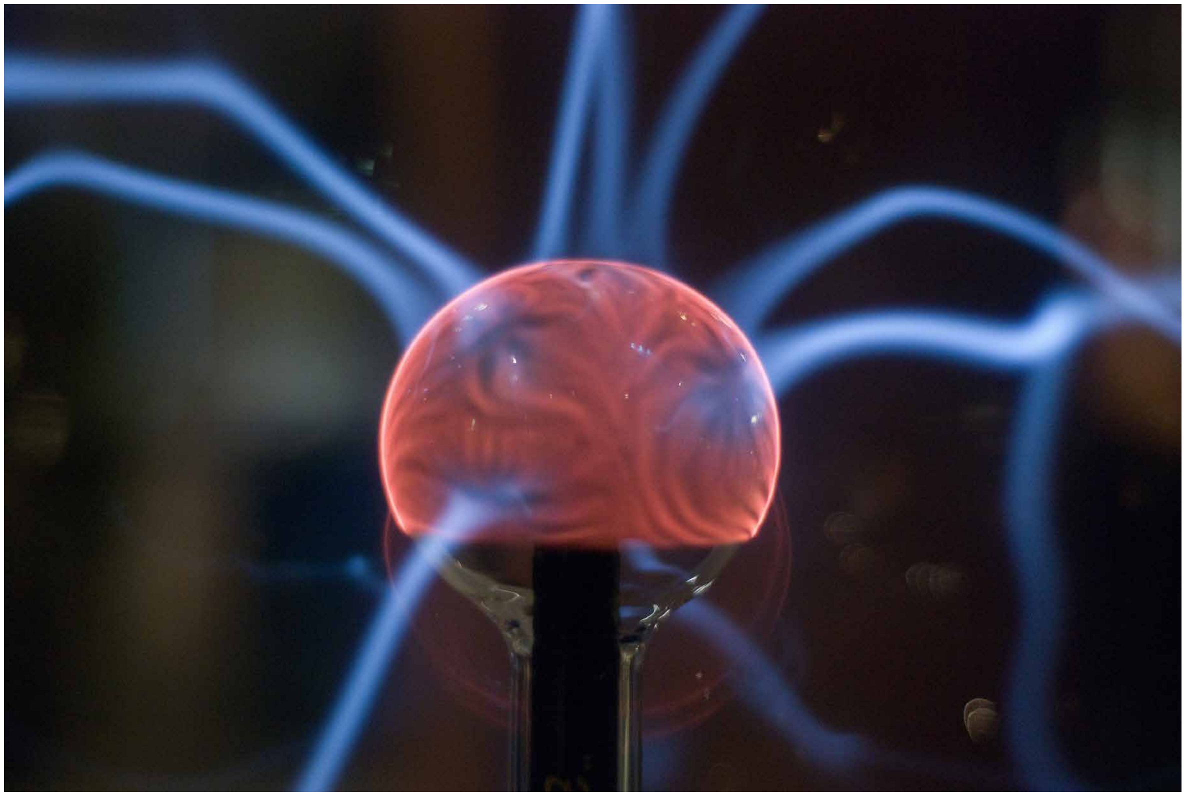
Another significant application of the blockchain technology lies in the know-your-customer (KYC) utility. The first Asian KYC utility led by HSBC, MUFG and OCBC, now at the "proof-of-concept" stage, was launched in Singapore last year.

The KYC utility in Singapore seeks to allow the banks in the consortium to share customers' information so that when a customer who has an existing bank account with, say, HSBC wants to open an account with OCBC, the former, upon obtaining the customer's consent, will be able to provide the latter with the customer's information. Even then, the banks in the consortium still need to work within the confines of the rules, Chia said.

Menon pointed out the need for distributed ledger technology to follow a set of standards, notwithstanding that it increases transparency and efficiency as well as reduce cost and risk.

DATA GOVERNANCE

The wider use of technology has raised awareness about the importance of data protection, which in turn requires strong data governance and management. Banks are now looking into how they can improve data governance, including how best to ensure accuracy of data for regulatory reporting purposes and business use such as to gain better customer insight, and for purposes of risk analysis, Chia said.



Artificial intelligence – are there sufficient protections for consumers?

Niall Coburn, Senior Regulatory Intelligence Expert, Thomson Reuters

The use and development of artificial intelligence (AI) applications and platforms is taking off at pace, presenting opportunities for companies in all areas of business.

Due perhaps to the speed with which the applications have been developed, there is scant regulatory advice about what "good" AI governance and oversight looks like. In a recent discussion paper entitled, "Artificial Intelligence (AI) and Personal Data – Fostering Responsible Development and Adoption of AI", however, the Personal Data Protection Commission Singapore (PDPC) provided some advice for establishing an accountability framework for such applications.

AI GOVERNANCE AND REGULATIONS

The PDPC pointed out the need for an appropriate approach to AI governance; one which still allows technology to develop without too many prescriptive rules. Artificial intelligence developers will nevertheless need more clarity about regulations so that AI can be efficiently developed and translated into different solutions. The paper said that, as AI systems develop, "explainability" will be a baseline requirement, and said it thought many regulators had yet to catch up.

The paper said that, when AI enabled decision-making applications were introduced, organisations should ensure there was transparency around the process, to increase consumer confidence and build public trust.

The paper said organisations should have a governance framework to be in place. Two basic components are needed to protect consumers:

• Decisions made by, or with the assistance of, AI should be explainable, transparent and fair so that affected individuals will have confidence in those decisions.

• AI systems, robots and decisions made using AI should be human-centric so that the design resolves around customer needs.

One issue that has already arisen for example, is the use of AI algorithms and models in decision-making systems such as "robo advice". The financial sector needs to ensure that the way these systems are used is transparent.

PROPOSED GOVERNANCE FRAMEWORK

The PDPC paper explored the type of governance framework that may be required to govern AI applications and recommended a four-stage process for organisations when establishing a such a framework:

• Define the objects of the AI governance framework.

• Select appropriate organisational governance measures.

• Consider consumer relationship with management processes.

• Build decision-making and risk assessments.

At the least, organisations must to be able to explain and verify the functions of the AI engine and confirm that it is performing to the expectations within the "technical and ethical perimeter set". If an organisation is providing an AI platform for financial products, it will need to give consumers assurances that the decision-making process being considered is adequately supervised and is working in their interests. It will also need to consider how the "paper trail" for AI solutions will work, how that will be reviewed and how it can be verified for regulators.

As the use of AI systems becomes more widespread, organisations will have to consider how their existing corporate governance needs to adapt and how their new responsibilities are being factored into the overall governance framework.

RISK AND HARM MITIGATION

Firms will also need to identify any potential risk or harm that may foreseeably arise from the use of such systems. For example, if a bank introduces a new AI teller machine, this will have to interact with anti-money laundering and customer data requirements, and there will need to be a review capability to ensure the system caters for regulatory and customer expectations.

There have been plenty of examples in the financial sector of such systems going wrong, with serious implications for the reputation of the organisation concerned. Other considerations include sampling assessments, documenting risks and reviews, data accountability and the ethical aspects of the overall risk.

CUSTOMER RELATIONSHIPS AND RISK

Artificial intelligence is normally introduced to improve efficiency and provide better services to customers. Part of the answer to the question of what "good" looks like in terms of AI systems must therefore be a consideration of the impact on customer trust and confidence.

The organisation will need to establish its policy for disclosure should things go wrong. Increasing transparency will help build customer confidence.

MAS requires tighter customer verification following cyber attack

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

The Monetary Authority of Singapore (MAS) has directed financial institutions to tighten their customer verification processes and assess the risk impact of the cyber attack at SingHealth from which personal information of 1.5 million individuals was stolen.

SingHealth is the largest group of healthcare institutions in Singapore which operate four public hospitals, give specialty centres and nine polyclinics. Following the attack, the MAS has expressed concern that the information stolen from SingHealth may be used illegally for carrying out unauthorised financial transactions.

MAS last week asked financial institutions not to rely solely on the information stolen, namely, name, identification card number, address, gender, race and date of birth, for customer verification purposes. It now requires financial institutions to request additional information for verification before undertaking transactions for customers. Additional information may include, among others, one-time password, pin, biometrics, last transaction date or amount.

MAS is also concerned about the impact of the SingHealth attack on financial institutions. It has required them, in light of the incident, to conduct a risk assessment of their control measures for the financial services they offer to customers, such as transaction and inquiry functions.

"Financial institutions are to take immediate steps to mitigate any risks that might arise from the misuse of the compromised information. MAS will engage financial institutions on their risk assessments and mitigation step," MAS said in a statement released on July 24.

VULNERABILITIES RELEVANT TO FINANCIAL SERVICES SECTOR

MAS' concern is valid given that the vulnerabilities in the health sector are relevant to the financial services sector, said David Copland, consultant at Bovill in Singapore.

"Social engineering and the technical 'man in the middle' attack to get customer security credentials still abound. Relying on just internal cyber security awareness is not sufficient; banks should seek out sources of know-how. For example, many consultancy firms have lists of current threats and vulnerabilities that apply to their business," he said.

Any data breach involving consumers' personal information exposes them to the risks of financial fraud, said Kunal Sehgal, executive director APAC at Financial Services – Information Sharing and Analysis Centre in Singapore (FS-ISAC). Such risk is mitigated by the fact that financial institutions in the city-state already have multiple layers of security in place to protect their customers, such as mandatory use of two-factor authentication and sharing of threat information in the financial services sector, he said.

UNDERSTANDING YOUR VULNERABILITIES AND POTENTIAL NATURE OF THREATS

MAS and global regulators have been constantly requesting financial institutions to perform cyber security risk assessments to establish the threats they face and any vulnerabilities across people, process and technology, according to Copland. This requires putting cyber-security investment in the right areas, based on an understanding of where the most vulnerable areas are and the nature of threats.

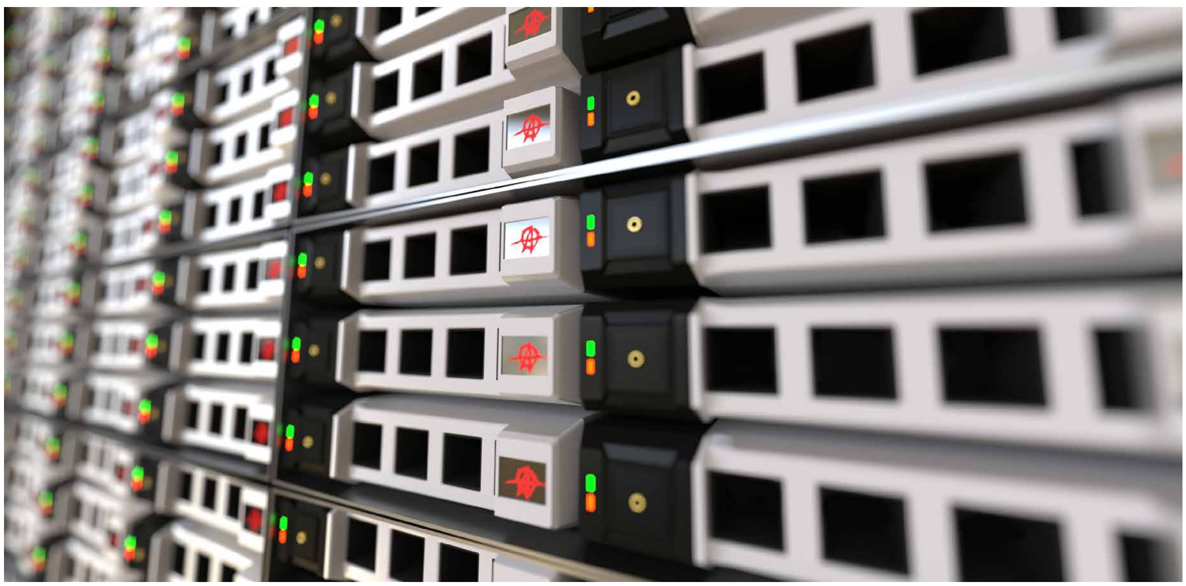
Be it the front office or the back office, cyber criminals will use various techniques to attack, Copland said. This could involve the use of social engineering to get information on account security credentials from an unsuspecting person and then access an account to commit fraud or steal other information, which is then used in an external hacking attack, he said.

"A common trick is to ring a client of a trading system up and represent the trading company asking for security details saying there has been suspicious activity on their account. It's surprising how when people are alarmed or frightened they will provide the attacker confidential information," he said.

MOST SUSCEPTIBLE AREA

Often attacks can occur during attempts to improve security. Copland cited internet trading offered by some financial services firms as an example, where in an attempt to make things more secure, firms can inadvertently disclose information which cyber criminals can use. For instance, asking customers to change their password regularly can be part of a script used by cyber criminals to social engineer customers in a phone call, he said.

"Criminals may find the username and customer's sign-in on the trading system, which is often just guessing their email address or finding their phone number. They then ring up and say something like: 'you have not changed your password for a while. Could you do this?' The criminal then offers validity by talking sensibly about the company and the trading system in order to make the customer comfortable to part with confidential information," he said.



PEOPLE THE WEAKEST LINK

Copland also pointed out that people are almost always the weakest link. This is evident from the fact that information useful to cyber hackers often comes from third-party service providers, internal staff, and internal processes.

"Internally, financial institutions do not mitigate cyber risks correctly often due to an oversight. While financial sign-off procedures are commonplace, it is not so for IT systems. Customers are susceptible to social engineering since they are not well trained in the social engineering threats and for that matter internal staff of the financial institution concerned," he said.

CYBER SECURITY SYSTEMS NEED BEEFING UP

Many financial institutions, however, have not done enough to beef up their cyber security systems despite the various attack incidents in recent years, said Copland, adding this explains the persistence of cyber attack. Those attacks include the $81 million heist at the Bangladesh central bank in 2016; the SWIFT hacking incident of Taiwan's Far Eastern International Bank in September 2017 which saw the loss of $60 million; the worldwide WannaCry ransomware attack in May 2017, and account takeover attacks leveraging global payments systems.

Financial institutions need to ensure they are not only on top of their cyber security technology such as anti-malware defence, ransomware defence software, intrusion detection and technology threat intelligence, but also people and process type of security risk mitigations to assess the presence of rogue employees, to segregate process duties, and to carry out staff recruitment checks, Copland said.

SHARING THREAT INTELLIGENCE

Large financial institutions now want to know what the latest type of attacks are, and there is now a greater desire among them to share threat intelligence. Many countries have formed various cyber-related fora such as CBEST in the UK and the Cybersecurity Fortification Initiative by the Hong Kong Monetary Authority (HKMA), and the Financial Services – Information Sharing and Analysis Centre in Singapore.

"There is also a trend for banks to now realise that internal people and process security is as important as something like technological defence, either internal or on the perimeter fence," Copland said.

While timely information sharing and transparency help all sectors to better combat cyberattacks, the onus is on consumers to remain vigilant and practise cyber hygiene such as checking their bank e-statements every month and reporting suspicious activity to their financial institutions, said Sehgal.

"They must also not click on suspicious links, while being mindful of not sharing any personal information publicly. We must continue to increase and evolve our security measures both as organisations and as individuals," he said.

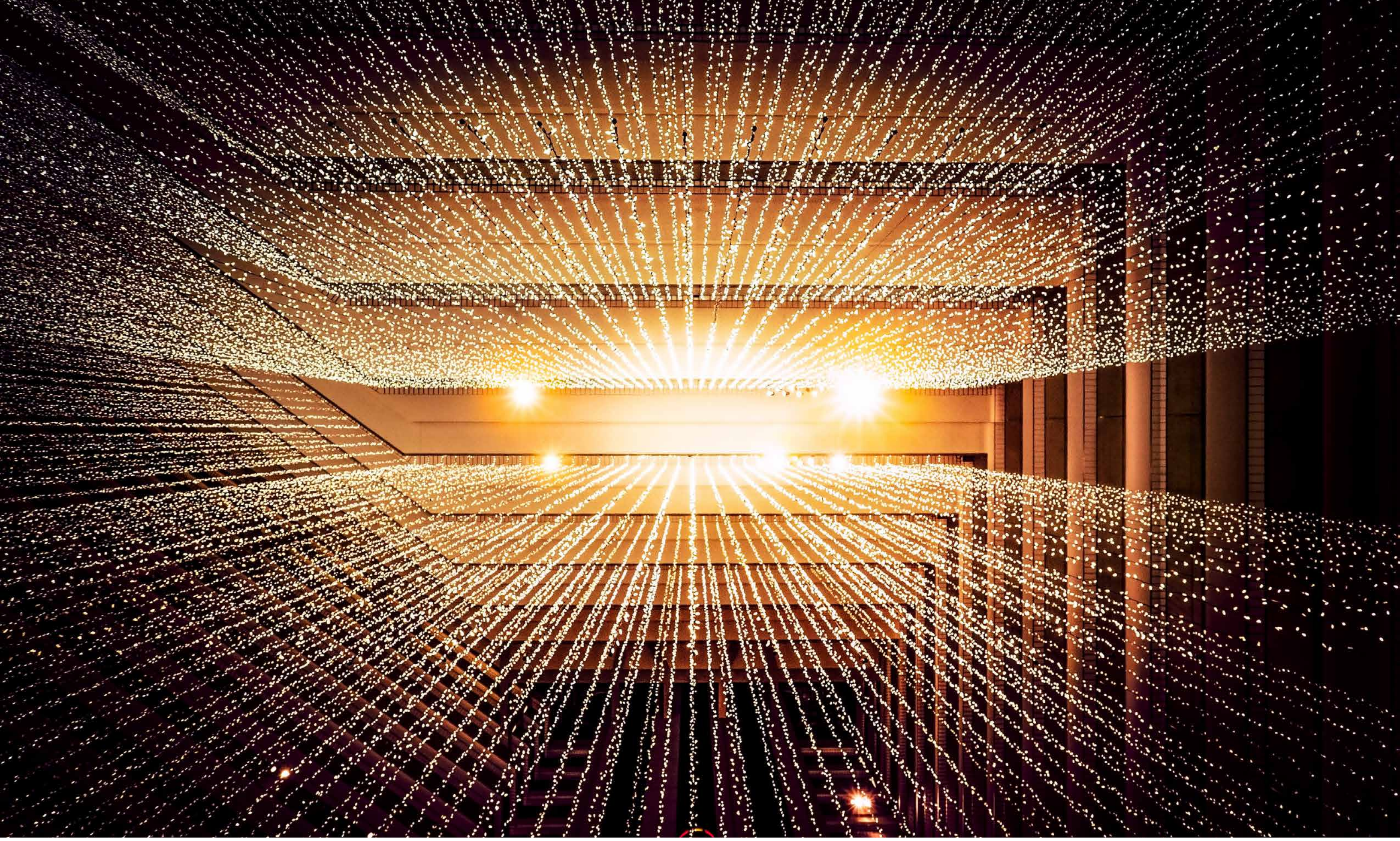
THE ROLE OF REGULATORS

While regulators have been active in their technology approaches for cyber security risk, they have not ventured far into tracking internal security risks, according to Copland.

"Out of 12 recent years of published large security breaches, the real source of 47 percent of the breaches was due either to internal staff or the wider enterprise, that is, customers, suppliers and outsourced service providers. For large financial institutions, this would be classified as internal risk," he said.

Regulators could consider focusing on reducing risk and require financial institutions to make significant auditable programmes on cyber risk reduction, citing recent cyber incidents, Copland said.

"In other words regulators should be looking for more than just having compliance officers tick a checklist against specific advice they give. Regulators need to bring in enforcement if there is a lack of auditable effort in cyber security projects. That is why you see the SEC prosecute not for the consequences of a cyber breach, but for not putting in sufficient measures in the first place," he said.



More Asian countries could follow Hong Kong's virtual banking initiative, questions raised

Patricia Lee, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

More Asian countries could consider implementing virtual banking as Hong Kong forges ahead with the authorisation of virtual banks but the industry is nowhere near to answering some of the questions raised, an official said.

The Hong Kong Monetary Authority (HKMA), in its "Guidelines on Authorisation of Virtual Banks", defined "virtual bank" as a bank which offers retail banking services through the internet or other forms of electronic channels rather than via physical branches. Virtual banks, which target mainly consumers in the retail sector and small and medium-sized enterprises, offer the prospect of financial inclusion, it said.

Simon Topping, regulatory partner at KPMG China based in Hong Kong, said many countries in Asia are likely to allow virtual banking so that more convenient customer services can be introduced, and access to financial services widened. In particular, with financial inclusion a high priority in developing countries in Asia, virtual banks could play an instrumental role, he said.

UNDERSTANDING THE REGULATORY IMPLICATIONS OF VIRTUAL BANKS

The future prospect of banking, enabled by technology, seems promising, some said. But others, such as Kevin Nixon, managing director of Nixon Global Advisory in Sydney, said the financial services sector is nowhere near to understanding the regulatory implications of a system that relies on virtual banking.

Banking systems are designed based on elements such as a physical infrastructure, with people running the operations, and having to comply with regulations such as capital and liquidity requirements and AML/CFT law. While virtual banking looks set to be the future of banking, a bank that provides banking services without an infrastructure raises some serious questions, Nixon said.

"I don't think we are near to understanding the regulatory implications of a system that relies on virtual banking. If your entire system is virtual, is that a desirable or manageable outcome? What does it mean in the next financial crisis? It doesn't mean that these questions cannot be answered but it's just that we are nowhere near to answering these questions just yet," he said.

VIRTUAL BANKS NEED TO MEET CAPITAL AND AML REQUIREMENTS

Notwithstanding their lack of a physical presence, virtual banks should be required to comply with all the regulations that have been imposed on traditional banks, including capital and AML requirements, Nixon said.

"These regulations are there for a reason: to protect the safety of the financial system, to prevent terrorist financing activities, and to protect consumers and investors. Do the current regulations necessarily apply in the right way to virtual banks? I come back to what I said earlier: we are nowhere near to having answers yet," he said.

OTHER ASIAN JURISDICTIONS AWAIT

Other Asian jurisdictions are now waiting to see how virtual banking works out in Hong Kong, including its impact on the financial sector.

The HKMA has received enquiries from approximately 50 companies since its announcement about Hong Kong's intention to promote virtual banking. Virtual bank applicants are grouped into four categories: traditional banks seeking virtual banking licences; Hong Kong fintech companies which are already involved in the lending business; telcos; and Chinese or overseas entities.

TOUGH EXPECTATIONS ON TECHNOLOGY

The HKMA is likely to choose some applicants from each of the four categories to try out different types of virtual banks, according to Topping. But he also pointed out the stringent criteria for virtual bank applicants, and in particular the regulator's expectations on their state of technology.

"The expectation on technology is so tough because their [virtual banks'] business is so heavily reliant on technology. They are expected to have technology risk management and contingency plans in place. It's not going to be straightforward to meet these requirements," he said.

In its guidelines, the HKMA specified requirements which potential virtual banks are required to meet before it would approve or reject an application. The regulator said it needed to be satisfied that the minimum criteria for authorisation in the Schedule 7 to the Banking Ordinance were met.

Some of the more significant requirements for virtual bank applicants include the need to put in place security- and technology-related controls, and to have their IT governance and systems independently assessed. Virtual bank applicants are also required to go through the eight types of risk (i.e., credit, interest rate, market, liquidity, operational, reputational, legal and strategic risks) identified in the HKMA risk-based supervisory framework.

Other requirements include the need for every virtual bank applicant to prove that it has a concrete and credible business plan setting out how it intends to conduct its business and how it proposes to comply with the authorisation criteria when conducting its business.

HKMA also expressed its concerns that a virtual bank might plan to build its market share at the expense of recording substantial losses in the initial years of operation, without any credible plan for profitability in the medium term.

"... a virtual bank should not allow rapid business expansion to put undue strains on its systems and risk management capability," the HKMA said.

BANKS HAVE ADVANTAGE MEETING HKMA AUTHORISATION CRITERIA

Unlike fintech players, traditional banks seeking a virtual banking licence will have a big advantage in terms of meeting HKMA's authorisation criteria, particularly in two areas, Topping said.

"One area [in] which fintech firms would need to meet the same standard as banks is AML. The second area is data security. These are the areas that banks are very experienced in. But for fintech companies they will have to meet HKMA's requirements in those areas," he said.

The success of virtual banks in Hong Kong could lead to a few scenarios including traditional banks setting up their own virtual banks or acquiring others, or working in partnership with fintech firms, Topping said.

Fintech set to feature high on Hong Kong's regulatory agenda in years ahead

Trond Vagen, Asia Editor, Thomson Reuters

Hong Kong's securities regulator faces a number of challenges relating to fintech and the online distribution of advice and financial products, a conference heard.

With the Securities and Futures Commission (SFC) set to release its conclusions to the May 2017 consultation on online platforms and robo-advisors, there are still questions that need to be addressed in areas such as cloud outsourcing and open banking, panelists said.

Last year's consultation focused on proposals to regulate online distribution and advisory platforms for investors, as well as how to apply suitability requirements which stem from old-style relationship management banking in an online environment. The rapid rise of fintech in recent years has lowered barriers for marketing to and servicing retail investors.

"[Fintech] is going to change the way in which financial services are being delivered," said Julia Leung, the SFC's deputy chief executive and head of intermediaries. "Some of the rules regarding suitability were written at the time when most of these products were being sold face-to-face. Now we certainly see a sea change coming in that area … we will apply our principles of investor protection when these technologies are being used. This means we will use the same principles to protect investors regardless of whether they are delivered face-to-face or in an online environment."

Speaking at the SFC Regulatory Forum in Hong Kong last week, she said the SFC was a "tech-neutral" regulator and that the consultation conclusions would be released soon. In addition, the regulator would put out a circular on the use of social media apps such as WeChat and WhatsApp for order placement, she said.

"In so doing we have to ensure that the key principles of record keeping have been observed, that there is a centrally controlled record, there is completeness, and there is security and compliance monitoring," she said. "We are looking into areas where we think we are able to do it."

Leung said outsourcing through cloud services was another area under study. She said there were potential regulatory compliance and enforcement implications surrounding the accessibility of cloud-stored data.

She said regtech and data analytics could help the regulator with its compliance testing, and that it had been using enhanced data analytics to detect compliance deficiencies.

"Our experience with firms is that it took them a lot of time in order to come up with a set of data which comply with our data standards," she said. "So we are embarking on a an initiative [with] the industry and developing a common industry standard for the format of trade-related data, so firms in future can use this to send their transaction data to us for compliance tracking and for detecting deficiencies and exception reports."

THREE CHOICES

Hong Kong faced three "big policy choices" with regard to fintech, said Andrew Procter, partner, financial services regulation at Herbert Smith Freehills.

"[Leung]'s consultation is completely in line with all the international stuff," he said. "Still, it begs some questions. Are you going to change the nature of the relationship down the manufacturing distribution chain? Are you going to put more emphasis and pressure on the manufacturers? That's happened in Europe under MiFID II; is Hong Kong going to follow, with all the implications that has for cost and liability?"

The second choice was whether the SFC would facilitate the use of cloud outsourcing and, if so, what level of due diligence and what access rights to information it would expect.

"What rights do you have to go in and find out what happened?" He said this could be a difficult dialogue to have with some of the largest offshore outsourcing providers, such as Google or IBM.

The third choice concerned how to approach open banking, he said. While the issue of open banking in Hong Kong is being consulted upon by the Hong Kong Monetary Authority (HKMA), its beneficiaries would largely be those regulated by the SFC, he said.

"If you can get better access to information from existing bank relationships and use that to structure your advice and make sure the product you're recommending is suitable and compliant, there is affordability for the product, you can close all sorts of advice gaps that currently exist and get a much better outcome for clients," he said. "You can also get a much worse outcome, because misusing that information could target the suckers."

Hong Kong could probably "jump in" at the same level of information availability as has been worked out under the European Union's Payment Services Directive 2 (PSD 2), he said, noting that Australia was now doing something similar.

Unless such information is made more available through open banking in Hong Kong, Procter said a likely outcome would be that tech giants such as WeChat would eventually use their customer data to begin offering targeted financial services to their users directly, and cut out the existing intermediaries.

REGULATOR EYES FINTECH APPLICATION USE

Tom Atkinson, the SFC's executive director of enforcement, said the regulator was also eyeing the use of fintech applications to improve market surveillance.

"Our surveillance systems are still pretty linear; they look for unexplained blips in the market," he said. "I don't think it's as sophisticated as it could be."

He said the SFC was considering whether to bring in big data to help with client identification and understand things on a more "comprehensive basis".

He said, however, that one problem faced by the regulator was that developing new tools in-house was a slow process, while partnering with third-party regtech providers was also not always the easiest process.

"The SFC itself has a fairly large data project going, where Keith Lui [SFC executive director with responsibility for the supervision of the markets division] is looking at systemic risk, [Leung] is looking at prudential risk and I am looking at conduct risk," he said. "The problem is, when we look at the available intelligence out there, there are so many new regtech firms you don't know what's bleeding edge."

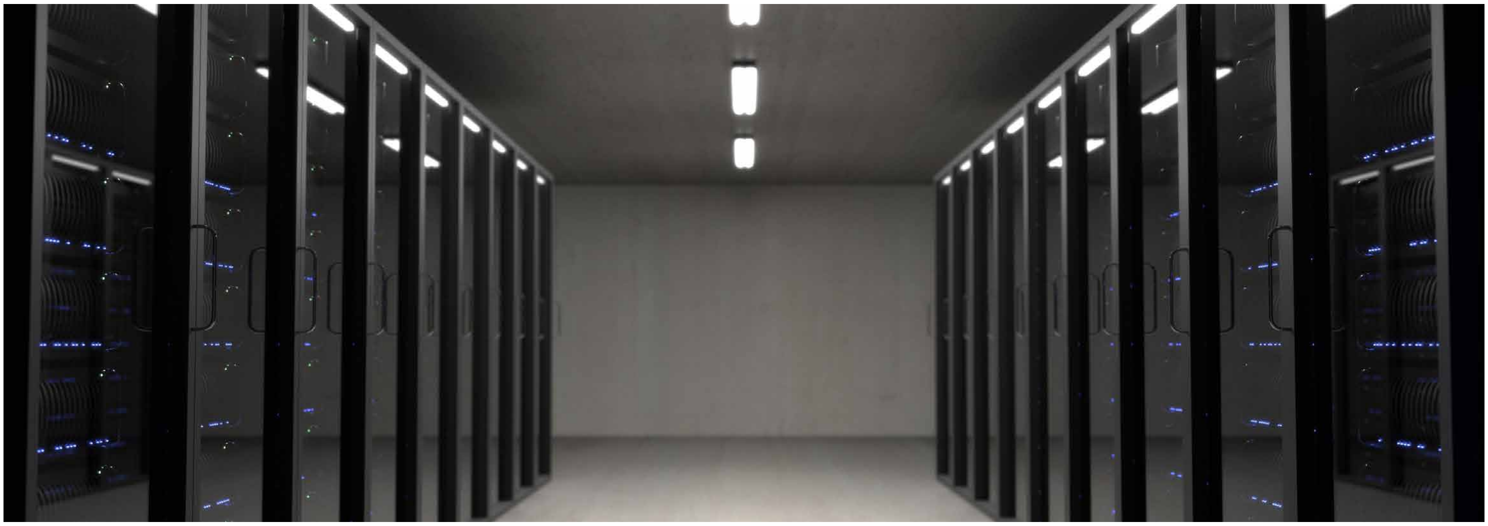
He said the regulator had picked nine conduct issues and asked itself what more information it would need to gain a better understanding of the problem.

"We are starting with the information we have within the SFC itself, looking at a project now to digitise that information and be able to read it," he said. After that, the SFC would seek to overlay market data on it.

"It's going to take a while but we could definitely do better in terms of intelligence," he said. "We know from all the other regulators in the world that they are all at this same point. Some are maybe 18 months ahead, but that's about it."

Procter, who has previously worked as a regulator at the SFC, the former UK Financial Services Authority and the former Australian Securities Commission, said other regulators were perhaps 18 months ahead in terms of expenditure, but not in success.

"A number of the bigger international banks have tried to do the same. They have all failed so far; the data isn't in the right form. They struggle to define what 'good' should look like except by working backward from actual breaches," he said. "They're all moving toward pulling together disparate bits of information that historically they have looked at in isolation. The best banks are the ones that have had the biggest rogue trading scandals, as you expect. In five years' time, they will give their traders wristbands and test their heartbeats, they will be able to see if they have crossed any Chinese walls, and so on. All of that will happen."



Hong Kong SFC aims to increase its use of technology under resource strain

Trond Vagen, Asia Editor, Thomson Reuters

Hong Kong's securities regulator is looking to use more technology to improve its supervision of the territory's financial markets after rapid growth in the number of firms it oversees has put a strain on its supervisory resources, an official said. Julia Leung, deputy chief executive of the Securities and Futures Commission (SFC), also said a trial run of data analysis performed on investment banks and brokers with high volumes in Hong Kong had yielded results it would otherwise have been unable to spot.

Given the rapid growth of technology-enabled businesses in the securities and futures industry in recent years, there has been a significant increase in the volume of trading data and the complexity of data relationships, she said. While firms are increasingly aiming to employ "regtech" solutions to manage compliance and costs effectively, the regulator was now examining how it could use more supervisory technology, or "suptech", to better police markets.

"With the assistance of technology, we have been able to identify irregularities, control deficiencies and non-compliance which would otherwise go undetected," she said.

Speaking at a conference in Hong Kong last week, Leung said the regulator's process so far had been slow, as firms needed to extract data from multiple systems and the data had to be consolidated, scrubbed, cleansed and validated for the SFC's use.

"To simplify this process, we are working with the industry, with the assistance of an external consultant, to develop a common industry standard prescribing the content and format of trading-related data to be kept by firms, which can be easily uploaded to the SFC's platform for analysis," she said. "The SFC has also established a data lab to conduct data analysis of high-volume data for compliance testing, surveillance and exceptional reporting purposes."

The growing interconnection between Hong Kong and Mainland Chinese markets in recent years has led to significant growth in the number of licensed corporations in Hong Kong. Leung said the total number of licensed corporations increased by 42 percent in the past five years to over 2,700 firms, putting a strain on the SFC's supervisory teams.

"This requires us to be more efficient and to use our resources wisely, focusing on areas which pose greater risk," she said. "To enable us to do the job properly, we need more data from licensed corporations."

The regulator was reviewing how it receives data through statutory returns from the industry, such as the Financial Resources Rules returns and Business and Risk Management Questionnaire. The SFC would soon soft-consult the industry on improvements in this area, she said.

"We are reviewing these and considering ways we can enhance data collection to heighten risk assessment and the use of data analytics."

Continuing market problems led to SFC's revised guidance on cooperation, says official

Trond Vagen, Asia Editor, Thomson Reuters

A steady stream of problems at regulated firms in Hong Kong was part of the reason the Securities and Futures Commission (SFC) decided to update its guidance on penalty reductions for cooperating with the regulator. In December last year the SFC said it would offer up to a 30 percent discount on enforcement penalties for firms that actively cooperated with its investigations, as part of a bid to speed up enforcement decisions and save resources.

"We are trying to move our resources to the more serious problems," said Thomas Atkinson, the SFC's executive director of enforcement. "You can do that in a number of ways: you can just close cases and take on more serious cases, or you can resolve those cases in certain ways and again focus your resources: this is one of the ways we think we can resolve things."

Speaking at the SFC Regulatory Forum in Hong Kong last week, Atkinson said the regulator's enforcement resources were being taken up by persistent minor or mid-level regulatory breaches by licensed firms in the territory.

"If you look at any big firm, most of the time they're going to have some regulatory problem ongoing," he said. "It could be a very minor problem or it could be a very serious problem, but there are a lot of ongoing problems as we move along. If they're willing to recognise that, put it behind them and remediate the problem, and if there's no client harm, or small client harm that has been remediated, we are willing to give them a discount off the penalty we would normally have imposed."

The cooperation route allowed the regulator to maintain a deterrent effect but also keep its "finite resources" focused on the bigger problems in the market, he said.

The revised guidance on cooperation with the SFC spells out three stages of an investigation at which penalties may be reduced from between 10 percent and 30 percent. It differs from the previous guidance, issued in 2006, which said that cooperation with the SFC might be rewarded with a disciplinary discount of a varying amount on a case-by-case basis.

Under the new guidance, firms approaching and helping the SFC from the initial detection of misconduct or regulatory failings up to the issuance of a notice of proposed disciplinary action (NPDA) would be likely to receive the full 30 percent discount. Meanwhile, a 20 percent discount would be offered to firms cooperating during the time from the issuance of an NPDA up to the deadline for the regulated person to make written representations in response to the NPDA. A 10 percent discount would be available to those cooperating from the deadline for making representations up to the issuance of a disciplinary notice.

Andrew Procter, partner at Herbert Smith Freehills and who has previously served as head of enforcement at both the former UK Financial Services Authority and the former Australian Securities Commission, told the forum the SFC's approach was similar to the regime in place in the UK, with a few exceptions.

"There is one big difference: in the UK, the clock starts ticking against you for the 30 percent discount only when the Financial Conduct Authority [FCA] tells you what its case is, in draft form," he said. "That does not happen here. It isn't always clear where the regulator ends up in an investigation."

He also pointed out that the Hong Kong regime does not allow reductions in cases involving individuals. "We're effectively talking about resolving matters at a corporate level," he said. "Individuals fight all the way, for obvious reasons."

ENFORCEMENT FIRST

Procter said there was a tendency for cases to go much faster to enforcement these days, a trend which had been exacerbated by the financial crisis 10 years ago.

"Things that historically would have been dealt with as supervisory issues went straight to enforcement for punishment," he said. "In the context of the financial crisis that is understandable. No doubt there was a need for some toughening compared to light-touch regulation and things that were fashionable leading up to the crisis."

He said there was "enormous tension" among senior management about whether incidents should be self-reported, amid fear that relatively minor cases would end up in enforcement.

Julia Leung, the SFC's deputy chief executive and head of intermediaries, said this was a misconception and that the SFC did not send "everything" to enforcement.

"If I go into an inspection where, through monitoring, we have discovered breaches and misconduct, of course there is a process in which I refer to [Atkinson]," she said. "But I would also ask: 'what is the best outcome for changing this behaviour?' If it is something regular, like risk management issues, then I will immediately go in and ask the company to undertake or impose licensing conditions to stop that behaviour. And that may be it."

TIMING

Peter Stein, managing director of the Private Wealth Management Association and the moderator of the panel, said there was some confusion in the market about the SFC's expectations on the timing of self-reports. Some firms may need first to ascertain whether or not in fact a material breach has occurred, he said, noting that under para 12.5 of the Code of Conduct the SFC requires immediate notification when there has been a material breach.

"Often a firm needs time to ascertain whether a breach is material and to get information on the matter," he said. Some firms feel that if they approach the SFC with a potential concern they want to discuss they may just be brushed off and told to self-report, he said.

Leung said early reporting, even if all the facts were not on the table, was a better option than reporting too late.

"We had a case where the self-report came to us after they spent one and a half years investigating, and when it came to us we were a little bit upset," she said. "I'd like to clarify that we do welcome early alerts, even if you do not have all the facts of the case. In most cases the firm would like to get to the bottom of it before reporting to us, but if it's 18 months later, that is not what our expectation is."

Atkinson agreed that early approaches were welcome. "I always tell firms … we'll look into it and if we find something we'll come back to you," he said. "It's very easy."

Hong Kong releases risk assessment report ahead of FATF inspection

Trond Vagen, Asia Editor, Thomson Reuters

Hong Kong's government has released the territory's first-ever national risk assessment for money laundering and terrorist financing threats, shining a spotlight on a number of recent regulatory and legislative moves to strengthen the AML/CTF regime. It also highlights areas of concern.

The report of the assessment comes less than half a year ahead of a scheduled inspection of Hong Kong's AML regime by the Financial Action Task Force (FATF), the international standard-setter. Publication followed consultation, quantitative and qualitative data examination and direct engagement with regulators, law enforcement agencies, government bodies and private sector entities, the government said.

Overall, the assessment ranked Hong Kong's ability to combat money laundering as medium high, with fraud the highest risk from both internally and externally. Other external laundering risks included drug-related offences, corruption, sanctions evasion and tax evasion, all posing medium high risk, the assessment said. Hong Kong was exposed to a medium high level of laundering risk, comprising a medium-high level of threat and a medium level of vulnerability.

"These threats arise from domestic activities and, to a greater extent, external activities due to Hong Kong's status as an international financial centre," said Carmen Chu, executive director of enforcement at the Hong Kong Monetary Authority (HKMA).

"Money laundering and terrorist financing vulnerabilities exist in various segments and banking products/services, including private banking, trade finance, international funds transfer, and retail and corporate banking."

Local and cross-border money launderers have exploited the high degree of free trade and strong financial and banking systems in Hong Kong and the report pointed to corporate bank accounts and money service operators as common conduits exploited by laundering syndicates.

Furthermore, the easy formation of shell companies was singled out as a risk, with trust or company service providers (TCSPs) being used by transnational syndicates to launder proceeds of crimes committed outside Hong Kong. Illicit gains were placed commonly in bank accounts, real estate and stocks.

For terrorist financing, Hong Kong was assessed to have a moderate level of terrorism threat, a medium-low level of terrorist financing threat, and a sound CTF framework in general. Hong Kong has no confirmed case of terrorist financing.

"High-risk patterns commonly associated with terrorist financing, such as abuse of non-profit organisations or physical movement of large quantities of currencies and bearer negotiable instruments across boundaries are not observed in Hong Kong," it said.

LEGISLATIVE MOVES

During the course of the assessment, some gaps in the territory's AML/CTF legislation compared to the FATF recommendations were identified and have since been addressed, the report said.

This resulted in the changes to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, which were implemented on March 1, under which legal and accounting professionals, estate agents and TCSPs are subject to the same set of customer due diligence and recordkeeping requirements as financial institutions.

The territory is introducing an ordinance targeting the cross-border movement of money, as set out under FATF recommendation 32. Known as the "Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance", or R32 Ordinance, this legislation becomes effective on July 16 and will establish a declaration and disclosure system to detect the cross-border movement of large sums of currency and bearer negotiable instruments into or out of Hong Kong.

The government is working to address gaps in the fulfilment of United Nations Security Council Resolutions. As part of this amendments have been introduced to the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) to prohibit any person from dealing with specified terrorist property and property of specified terrorists or terrorist associates, and to criminalise the financing of travel between states for terrorism-related purposes. These amendments will come into operation on May 31, 2018 as the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance 2018.

Hong Kong is aiming to amend the United Nations Sanctions (Democratic People's Republic of Korea) Regulation, the report said. In the meantime, the government has told the various financial sectors of sanction measures and reminded them not to engage in or facilitate activities related to North Korea, and to conduct continuous screening.

"The government is committed to combating money laundering and terrorist financing together with the international community," a government spokesman said.

"As part of our ongoing efforts to strengthen the regime, we have conducted this risk assessment to facilitate the formulation of more targeted responses. Our AML/CTF regime has been reinforced further with the enactment of four pieces of primary legislation in the past year to address the identified risks."

LOOKING AHEAD

Aside from legislative moves, the report identified strengthening risk-based supervision as a priority, including a stronger partnership between law enforcement agencies, regulators and the financial intelligence unit.

The report highlighted the recent engagement between the private sector and the HKMA in combating money laundering through the police-led Fraud and Money Laundering Intelligence Taskforce (FMLIT). This public-private partnership allowed for the discussion of cases, trends and typologies and the sharing of intelligence, contributing to a shared understanding of risks. The government was considering expanding the platform after more implementation experience has been accumulated, it said.

In a recent speech, Arthur Yuen, the deputy chief executive of the HKMA, said the FMLIT had resulted in the freezing or restraint of some HK$2.8 million as well as 71 arrests over a 10-month period since its inception last year.

The report also highlighted outreach and awareness-raising efforts by the government and regulators, as well as the need to monitor emerging risks such as virtual commodities. The police would also step up its use of financial intelligence and international cooperation to fight money laundering, the report said.

"Authorised institutions should study the report carefully, consider the relevant insights and implications, and review and update, where appropriate, their own institutional ML/TF risk assessments accordingly," Chu said.

The HKMA will organise an industry seminar on June 11 to discuss the findings of the report and banks should nominate senior representatives such as money laundering reporting officers, heads of legal and compliance or other managing staff to attend, Chu said in a circular.

Hong Kong securities regulator to revamp anti-money laundering guideline ahead of FATF visit

Trond Vagen, Asia Editor, Thomson Reuters

Hong Kong's securities regulator want to make it easier for financial institutions to use technology to onboard customers ahead of a counter-money laundering inspection by the Financial Action Task Force (FATF) later this year.

The Securities and Futures Commission (SFC) also proposed in a consultation to expand the types of politically exposed persons (PEPs) to be covered under the territory's AML regime to include customers who have been entrusted with a prominent function by an international organization such as the United Nations or World Trade Organization.

If enacted, the proposals would amend the SFC's Guideline on Anti-Money Laundering and Counter-Terrorist Financing to keep it in line with international anti-money laundering and counter-financing of terrorism (AML/CFT) standards. The SFC said it would also be more useful and relevant.

Hong Kong is due to undergo a mutual evaluation by the FATF in October this year and its regulators have said AML/CFT reforms are a priority ahead of the visit. In early May, the government released its first-ever national risk assessment for money laundering risks, highlighting areas where the territory's AML regime needed to be improved, such as the cross-boundary movement of funds and sanctions compliance.

In its consultation, the SFC proposed to streamline the identification and verification processes for onboarding customers, thereby allowing firms to adopt "reasonable risk-based measures" to verify customers' identification information. It said firms could use technology for non-face-to-face account opening if they could ensure and demonstrate that there are adequate safeguards against impersonation risk.

"The SFC is committed to adhering to international AML/CFT standards to reinforce Hong Kong's reputation as a major international financial centre," said Ashley Alder, the SFC's chief executive. "In formulating the proposed amendments, we adopted a balanced regulatory approach to give firms flexibility while ensuring our requirements are effective to prevent money laundering and terrorist financing."

The consultation is open until August 9, 2018.

PEPS AND TECH

The SFC noted that the FATF has strengthened its standards in several areas identified as high risk relating to PEPs to address concerns about corruption.

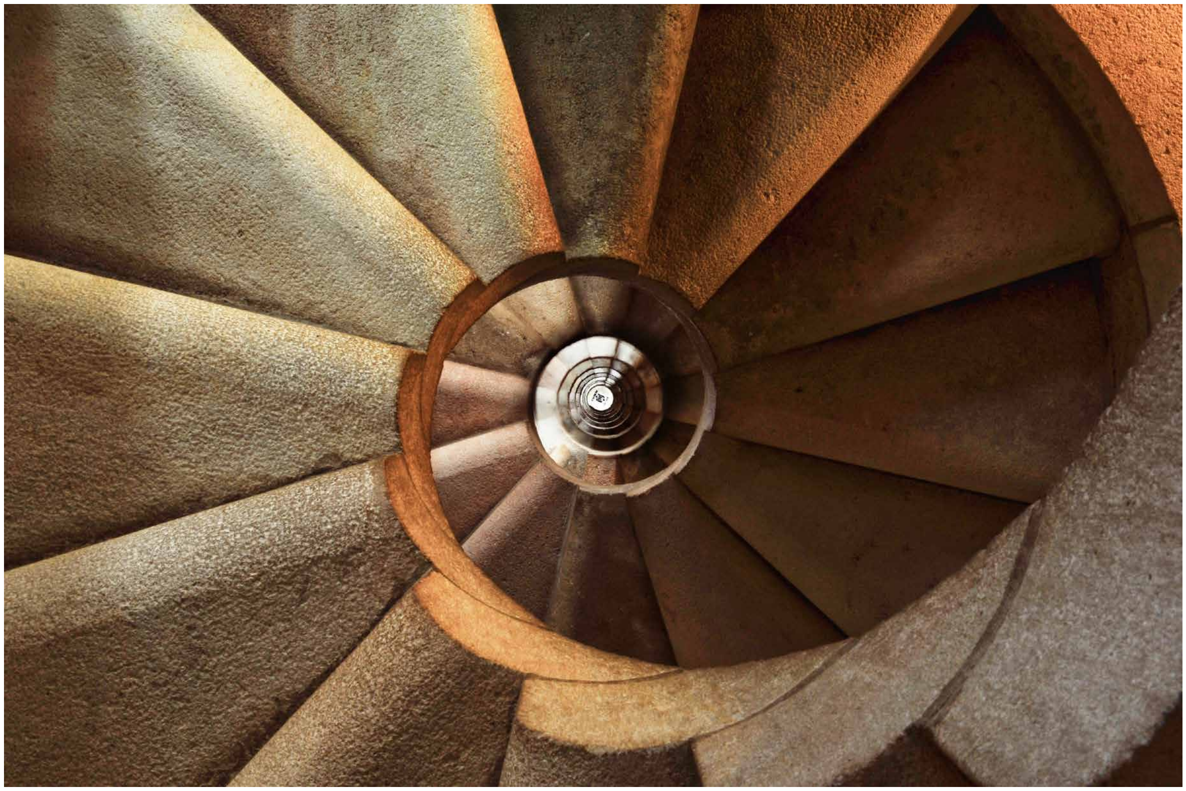
The SFC's proposals included expanding the types of PEPs covered by the guideline to include persons who have been entrusted with a prominent function by an international organization such as the UN, and extend the special requirements for foreign PEPs to high-risk business relationships with domestic PEPs and international organisation PEPs.

The regulator is also proposing to allow firms to implement group-wide AML/CFT systems in all of their overseas branches, including information sharing.

Firms would also have to identify and assess money laundering or terrorist financing risks that could arise from the use of new technologies, the SFC said.

Furthermore, firms would be allowed to stop pursuing customer due diligence processes if they reasonably believe that performing the process will tip off the customer, but with a requirement that the firm file a suspicious transaction report (STR) to the Joint Financial Intelligence Unit (JFIU).

The SFC's proposals also include a requirement that firms keep all records obtained throughout the customer due diligence and ongoing monitoring processes.



2018 salary survey: AML roles stand out in otherwise cautious Hong Kong market

Trond Vagen, Asia Editor, Thomson Reuters

Anti-money laundering (AML) compliance positions will be in high demand in Hong Kong during the year ahead, recruiters said. Financial institutions are aiming to bolster their AML credentials as the territory prepares for a mutual evaluation by the Financial Action Task Force (FATF).

The Securities and Futures Commission's (SFC) Manager-in-Charge (MIC) regime has also increased demand for experienced compliance professionals, particularly among smaller firms and funds, they said. In addition, the rising number of mainland Chinese companies setting up in the territory has led to demand for candidates with strong or native Mandarin skills.

Meanwhile, on the fringes of traditional finance demand is also booming for compliance personnel: a sizeable influx of firms dealing in cryptocurrencies has led to a need for individuals with regulatory experience.

In its annual compliance salary survey for Asia, Thomson Reuters Regulatory Intelligence has collated responses from recruitment firms on some of the main issues facing the industry, as well as salary trends and expected demand for compliance personnel in the years ahead.

Overall, the picture painted by the replies was one of a market gently slowing down from its hiring heyday following the 2007/8 financial crisis, but with pockets of high demand for professionals with certain skills. Salary increases and bonus payouts were roughly in line with recent years and can be found in the table at the end of this article.

AML PERSONNEL STILL IN DEMAND

Financial crime and AML roles remained in consistent demand last year and this will continue through 2018 with Western, local and mainland Chinese banks aiming to add talent in this area, said Edward Chen, director at Harbridge Partners in Hong Kong.

"For some global firms, due to recent enforcement actions there has been a keen desire to strengthen transaction surveillance and monitoring, equities and derivatives products compliance. [There has] also [been demand for] regulatory compliance and regulatory risk professionals that deal with internal regulatory risk," he said.

Regulatory liaison professionals with experience of dealing with regulators on enquiries, investigations and potential enforcement matters were also sought-after, Chen said. This area may prove important in the coming years as the

SFC has shown renewed interest in resolving cases at an early stage by offering penalty discounts for active industry cooperation.

The regulator has also prioritised the pursuit of corporate fraud, and this too has had an impact on recruitment for roles in AML, said Rob Green at GRMSearch.

"Activities such as AML/CTF compliance continue to be a priority and disciplinary actions such as sanctions, fines and bans are robust to ensure active deterrents," he said.

Many banks started to build out their financial crime compliance (FCC) teams late last year, and that trend has carried on into 2018, said Amy Ho, director at Ambition.

Hiring has also continued to be buoyant across junior- to mid-level roles in know-your-customer (KYC) and customer due diligence (CDD), she said.

"The market is more active in the AML/financial crime compliance space among the international banks," she said.

"Most of the core compliance, regulatory compliance and markets compliance advisory roles are replacement roles only, whereas in the AML/FCC space [they] are able to get new headcount."

FURTHER ROLES IN DEMAND

While the legal and compliance functions have traditionally been separate from one another, there is increasing demand for compliance personnel with legal experience, some recruiters said.

"We have seen a big uptick in positions where both legal and compliance functions are merged and now require candidates to manage both sections of the business," said Sid Sibal, associate director at Hudson Hong Kong's financial services practice.

"As an example, we see a large number of roles titled 'legal and compliance manager'. Also, employers are starting to focus more on candidates who have LLBs or [other] legal qualifications."

The MIC regime, which came into effect last year, has forced firms in the territory to map out their senior management structure and appoint "managers-in-charge" for several business lines. While the SFC has said it is pleased with the effect the regime has had on the market, it has also had an impact on the dynamics of compliance recruitment, particularly in the asset management sector.

"We had a number of funds looking at hiring within compliance to accommodate the SFC's requirements for the MIC regime," said Tony Wilkey, senior consultant at Robert Walters in Hong Kong.

"Funds that had historically run a COO-only management structure brought on general counsel or chief compliance officers; coupled with the MIC this was also in respect to investors and [limited partners] (LPs) becoming more concerned with compliance risk and desiring to have an independent dedicated resource in this space."

There has also been an increase in new small asset management firms being set up in Hong Kong, and these companies are looking for senior compliance candidates to work as a one-person compliance team and be the MIC for the company, said Janae Chan, managing consultant at Ambition.

"Candidates with equity compliance or product compliance experience are popular among the asset management firms too," she said.

TECH ROLES

With Hong Kong attracting a steady number of cryptocurrency startups, several recruiters said those firms wanted to hire compliance staff for technology and governance positions requiring knowledge of cryptocurrencies.

"We see a lot of crypto exchanges and cryptocurrency investment companies opening up shop in Hong Kong and that increases the demand for candidates who have a strong interest in this new space," Sibal said.

A relatively new area of compliance hiring was for "technology risk professionals" with experience in analysing, identifying and solving trading platform or technology-caused software lapses or breaches, Chen said.

"There is growing interest from global firms in exploring and utilising technology to automate manual and repetitive tasks, and a focus on fintech or regtech compliance," he said.

"Top-tier global firms are also examining the risks and impact of blockchain technology and how providers of cryptocurrencies and other technology-driven payment exchanges and platforms could impact their business, and the implications of how compliance and regulation can be applied to safeguard user interests on these new platforms."

Chen said he expected to see a rise in demand for "tech-savvy professionals" with a deep understanding of how technology can automate or solve compliance risk issues.

Ho expected to see more roles outside traditional compliance functions requiring data analytics skills, especially in monitoring, testing and surveillance roles.

THE MAINLAND CONNECTION

Recent years have seen strong growth in the number of mainland Chinese firms setting up in Hong Kong, as a result of the growing interconnection between the two markets. According to the SFC, the total number of licensed firms rose by 42 percent in the past five years, to more than 2,700 firms. This rise in activity has also been reflected in the recruitment market, Chen said.

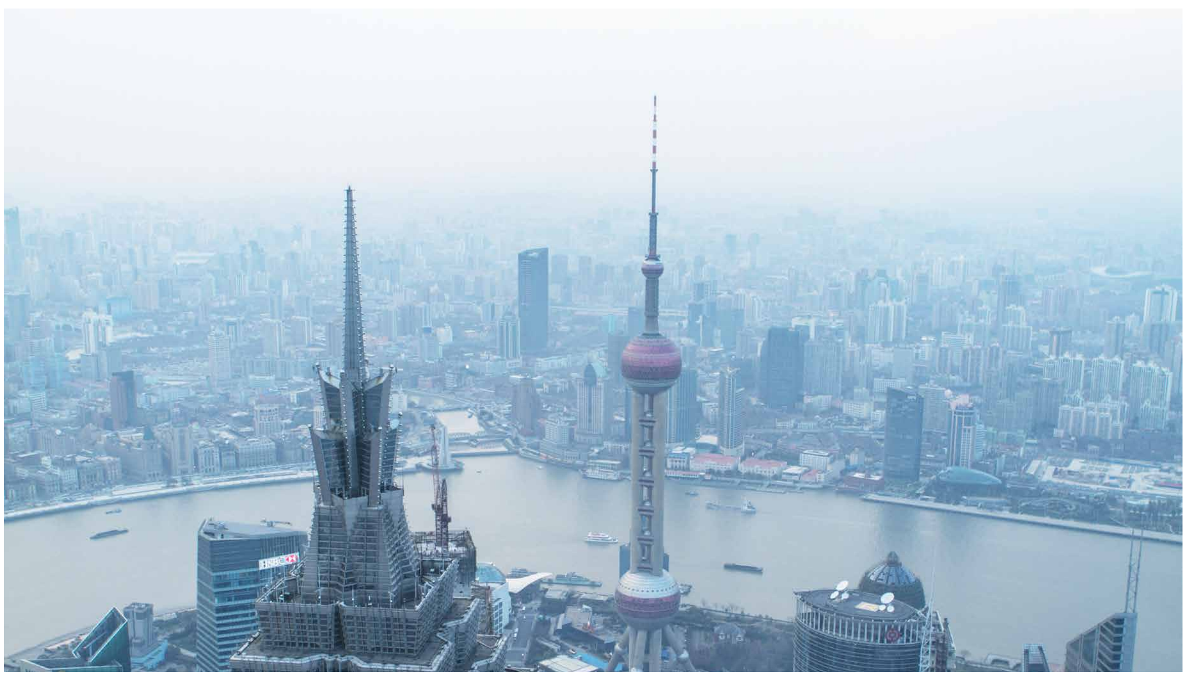
"Many of the vacancies we have been working on in the last year from mainland and local firms have been from integrated securities houses with SFC licensed types 1,2,4,6 and 9 regulated activities," he said.

candidates' ability to "understand mainland business culture" and to communicate effortlessly with senior management in China, Chen said.

There was also high demand for multilingual candidates with strong English communication skills but who could also liaise with various regional regulators in their native language, such as Mandarin for the China Securities Regulatory Commission and Cantonese for the SFC, Wilkey said.

KEY SKILLS

Recruiters said some trends from previous years had continued, and become more commonplace, such as the tendency to "juniorise" positions that become open to try to reduce salary costs. A role previously held by a departed senior vice president may instead be put on the market as an associate vice president, often with added responsibilities. Some also chose to not recruit for vacant headcount and instead promoted junior staff internally as a cost-saving measure, they said.



"Fluent Mandarin-speaking compliance professionals with experience such as cross-border corporate finance, DCM and syndicated finance exposure are sought-after skill sets. Similarly, cross-border asset management and investment funds compliance professionals with a mainland background have been able to secure multiple job offers."

Mainland firms were keen to secure native language compliance talent in Hong Kong because of the

There were certain skills and backgrounds that would help candidates in the 2018 recruitment market, however, recruiters said.

A strong educational background, such as a law degree, was always a desirable asset for a candidate hoping to secure a role in compliance, Sibal said. At mid- to senior level, clients often preferred candidates with legal qualifications such as a Master of Laws (LLM), Ho said.

Norris Wong, senior consultant at Hays, said candidates with strong business acumen and the ability to find business-oriented yet compliant solutions for institutions would be sought-after.

Strong organisational skills, risk assessment capabilities and effective communication skills were desirable in compliance candidates, Green said. The ability to see the bigger picture and analyse information was also important as it helped minimise risk and prepare a firm for regulatory changes, he said.

A background in forensic investigation or law enforcement would be a useful asset for candidates considering fraud investigation roles, Chan said.

THE NUMBERS

Overall, salaries rose by annual increments of between 2 and 8 percent across the spectrum, with the exception of only a few very senior positions, Chen said.

"In fact, aside from salaries remaining [mostly] the same, we have noticed that when a role is made vacant, there is a tendency for firms to lower the salary budgets for replacement hires," he said.

Candidates were also wary of moving to a competing firm in the current market conditions, with some saying the "hassle" of looking for a new job was not worth the risk and potential pay rise in the new position.

"For many compliance professionals, job security, job satisfaction and work-life balance takes precedence to salary," Chen said.

"This could be because the Asia-Pacific and global economic situation is unpredictable, and there is a general acceptance by compliance professionals working for Western firms that salaries are roughly similar and that a lateral move for a 5-15 percent increment is unattractive and risky."

While most candidates typically would ask for a 20-25 percent pay rise to move to a new role, banks were generally reluctant to offer more than 15-20 percent, said Nishita Mohnani, senior consultant at Hays.

Salary expectations were "somewhat reasonable", with candidates having a fairly good understanding of market rates, Wilkey said. "There are of course a small percentage of candidates still expecting large increases of 30 percent or higher, but we find those professionals lack understanding of the market and firms have been less receptive to this than, say, three or four years ago," he said.

BONUSES

Bonus payouts were more or less in line with expectations and little changed from last year, the recruiters said. Another continuing trend was that mainland Chinese banks tended to offer bigger bonus payouts but lower salaries.

In general, junior- to mid-level compliance professionals received between one and three months' salary as bonus, while the more senior professionals were able to receive up to five months' salary as bonus, according to data from the recruiters.

"Average bonuses at the American and European banks sat at around one month across all levels, and within the larger regional banks in Hong Kong bonuses were at around two months," Mohnani said. "Chinese banks continue to pay out higher bonuses, with averages at four months."

Mainland Chinese firms, established Chinese securities houses and investment banks were rewarding well, as in previous years, whereas the track record at some smaller finance houses, including state-owned asset managers, was more inconsistent, Chen said.

There was also a trend for some of the newer mainland Chinese firms to pay their compliance staff deferred bonuses, typically spread over the course of a year or longer, he said.

"This is possibly a reflection and recognition of the importance and value of experienced and senior compliance staff by mainland and local firms, and bonus scheme payments are now designed to encourage loyalty or to commit staff to their employers," he said.

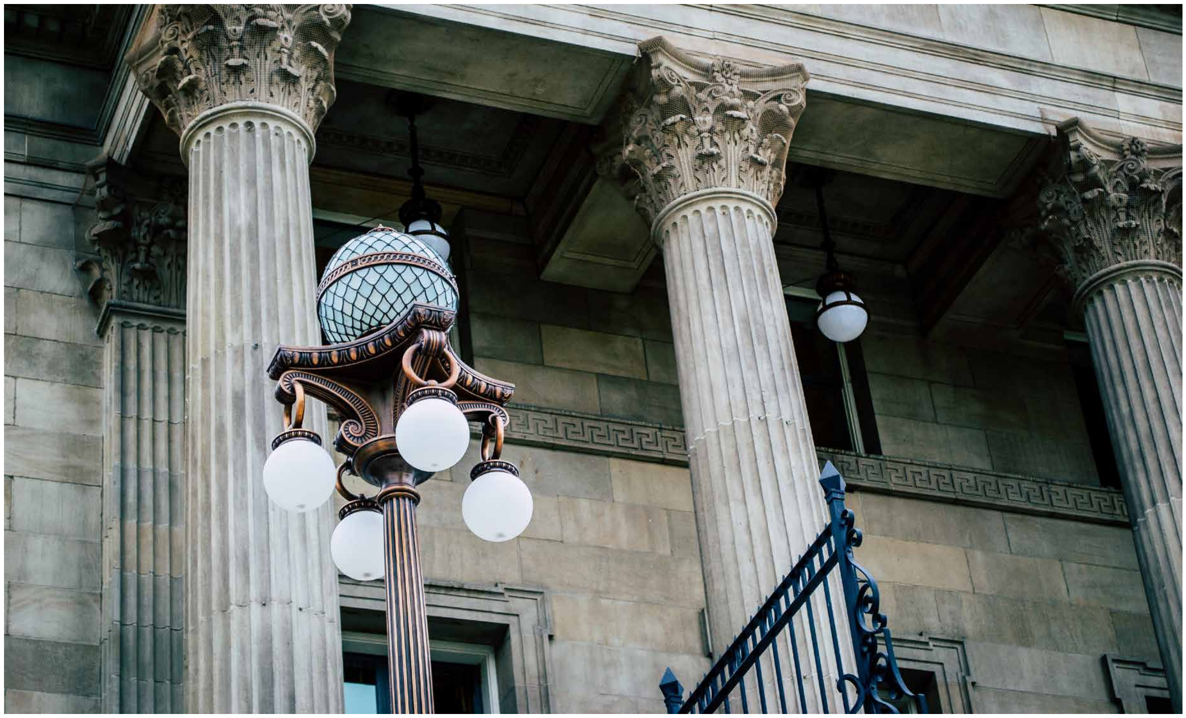
LOOKING AHEAD

The expectation of yet more regulation and enforcement activities on the horizon would not necessarily lead to an increase in permanent compliance vacancies, Chen said.

"The overall mood is one of caution, caution and caution in hiring, and in business activities in general," he said.

Recruitment volumes in compliance functions have decreased so far in 2018, compared with 2017, with most hiring taking place in the local banks and Chinese investment banks and securities firms, Ho said.

"However, we envision there will be more roles outside traditional compliance functions requiring knowledge of or experience in compliance, such as chief operating officer roles, first-line risk roles and regulatory and compliance change roles," she said.



AUSTRAC sees regtech innovation as critical in fight against financial crime

Nathan Lynch, Regional Bureau Chief, APAC, Financial Crime & Risk, Thomson Reuters

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is continuing to prioritise innovation in financial crime compliance with its support for initiatives to build a stronger regtech ecosystem in Australia. The financial crime agency will hold a "regtech showcase" tomorrow to bring together regulators, technology innovators, investors and reporting entities at the Sydney Startup Hub.

The initiative follows the AUSTRAC Innovation Hub and Smarter Regulation Program and is designed to create a collaborative environment where innovators can work together to use technology to solve complex financial crime challenges.

The showcase follows an announcement in March that Australia is forging stronger ties with the UK to build a "bridge" to allow fintech and regtech companies to passport their services. This coordinated approach would allow Australian innovators to tap into a larger ecosystem for their products, local regtech companies said.

Australia is home to the world's third largest regtech sector after the United States and UK. It has the right level of political and regulatory support but an immature market for investment and capital is holding back growth.

A number of regtech start-ups will demonstrate their products along with presentations from senior AUSTRAC officials. The event would "provide a platform for discussion around regtech capabilities and industry expectations," AUSTRAC said.

The event follows the financial intelligence codeathon that AUSTRAC hosted in March alongside the ASEAN-Australia Special Summit.

The establishment of AUSTRAC's Innovation Hub will ensure technology will play a critical role in combating financial crime. The agency is working on a number of high-level initiatives involving data lakes, advanced encryption and artificial intelligence to tackle key financial crime intelligence challenges. The agency is also playing a role in the CSIRO's Data61 initiative to build an open platform based on machine-readable laws, regulations and rules to simplify compliance.

The program, which builds upon 10 years of research and development, will aim to build the foundation of a new regtech industry powered by digital legislation.

TECHNOLOGY ESSENTIAL TO COMBATING FINANCIAL CRIME

On Tuesday more than 80 participants from banks, non-bank financial institutions, gambling and remittance providers, as well as industry bodies, AML service providers and regulators will discuss these opportunities and challenges.

"Technology-based innovations are critical in our fight against money laundering and terrorism financing. As Australia's regtech sector continues to grow, the extent of this development will depend on investment and support," AUSTRAC said.

AUSTRAC has also joined forces with the Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA) to foster the local fintech and "regtech" industry. Local officials aim to create the most successful regulatory innovation hub in the Asia-Pacific region.

Senior regulators are optimistic Australia's mature regulatory model and harmonisation with the world's major financial centres makes it a natural place for a regtech export industry. They want to create a climate in which businesses get the support and guidance they need to deliver products to domestic firms as well as the international marketplace.

ASIC is also pushing ahead with "digital regulation initiatives" in line with Data61's world-leading research. The conduct regulator is exploring the use of natural language processing (NLP) and machine-executable reporting to drive the industry forward.

ASIC also runs a sandbox for fintech firms and is also providing regulatory guidance to innovators that are aiming to launch products to address corporate and conduct regulatory challenges.

REGIONAL REGTECH HUB

The UK and Australia have the second and third largest markets in the world for regulatory technology, according to data from Boston Consulting Group (BCG). The consultants said that U.S. companies had access to the deepest funding pool by a wide margin, with 126 start-ups raising $1.6 billion in project finance. In the UK, 78 businesses have raised a total of $500 million, while in Australia 27 start-ups have raised a total of $100 million.

Regtech businesses have a different financing profile to fintech companies and typically find it harder to raise equity financing. The founders of regtech companies tend to be former practitioners and subject-matter experts, who often self-fund their ventures, BGC said.

On the plus side, regtechs tend to generate revenue earlier than fintechs whose primary focus is on customer acquisition. The regtech success stories tend to be acquired by the more mature enterprise risk solutions, the consultants said.

Meredith Ozeri, compliance manager at AUSTRAC, told a recent industry forum the Innovation Hub had supported 42 businesses to develop products for the local and international markets. AUSTRAC was careful to ensure its support of regtech businesses was not seen as an endorsement; instead, AUSTRAC provides a "negative assurance" to businesses in its Innovation Hub, Ozeri said.

Regulatory agencies and start-ups were looking at creative ways to address the funding challenge, as this would be critical to the success of the sector. This could include a combination of government incentives, support with pitches for procurement contracts or innovative self-funding models.

Julian Fenwick, chair of the RegTech Association, said Australia needed to work on collaboration and financing to allow the industry to succeed. The new approach would make it faster and cheaper for start-ups to get licensed in both jurisdictions.

The mutual recognition scheme is encouraging for the regtech sector, which is struggling to reach critical mass in the Australia, he said.

FUNDING CHALLENGES REMAIN

Despite this regulatory support, start-ups say it is a tough task to get products to market.

Anthony Quinn, co-founder of Arctic Intelligence and AML Accelerate, said businesses needed greater encouragement from regulators to have the confidence to use regtech solutions. Local companies wanted to embrace technology but were unsure whether this would satisfy the regulators, he said

"ASIC and AUSTRAC in particular have been active but it would be great to see more from them in supporting regtech providers," he said.

"Forming alliances with different regulators in different jurisdictions is a great start but I'm not sure it will be a 'shot in the arm' or help with capital raising."

Quinn said regulators would also benefit — with a better prepared regulatory population — if Australia has a healthy and diverse regtech sector. The anonymised and aggregated data from regtech providers could help regulators spot areas where more work needs to be done, he said.

"At scale they will have a massive challenge to ensure tens of thousands of businesses comply with AML laws. So regulators stand to benefit from tech providers as much as the regulated communities that they regulate," Quinn said.

FATF urges countries to target $150 billion global human trafficking trade

Nathan Lynch, Regional Bureau Chief, APAC, Financial Crime & Risk, Thomson Reuters

The Financial Action Task Force (FATF) has identified human trafficking, forced labour and sexual exploitation as predicate crimes where the financial sector can play a significant role in identifying victims and disrupting a $150 billion global criminal industry. The Paris-based financial crime standard setter said many countries were failing to keep pace with the development of human trafficking (HT) activities and financial indicators.

The FATF said in a new report that human trafficking and migrant smuggling were growing significantly as predicate crimes. The International Labour Organisation (ILO) estimates that forced labour generates $150.2 billion each year in criminal profits. In addition to the organised crime links, HT is increasingly being used to fund violent extremism.

The FATF said the displacement and vulnerability of people in conflict zones had led to a surge in HT cases, including the involvement of opportunistic terrorist organisations.

"In addition to the terrible human cost, the estimated proceeds that human trafficking generates have increased five-fold since the FATF produced a comprehensive report on the laundering of the proceeds of these crimes in 2011," the task force said.

Since that report, authorities have gained a better understanding of how and where human trafficking is taking place. There is an increasing prevalence of people being trafficked in the same country or region, the FATF said.

The latest FATF report was prepared with the assistance of the Asia-Pacific Group on Money Laundering (APG). Human rights groups estimate that the Indo-Pacific region has more victims of slavery and human trafficking than any other region in the world.

The report aims to raise awareness about the type of financial information that can identify human trafficking for sexual exploitation or forced labour and to raise awareness about the potential for profit-generation from organ trafficking. The report also highlights potential links between human trafficking and terrorist financing.

"As human trafficking can happen in any country, it is important that countries assess how they are at risk of human trafficking and the laundering of the proceeds of this crime, share this information with stakeholders and make sure that it is understood," the FATF said.

The global body is urging countries to build partnerships between the public sector, private sector, civil society and non-profit communities to tackle these threats.

"Financial institutions in particular, and non-profit organisations that provide support to the victims of this crime, are on the frontline and have a crucial role in tackling human trafficking and the financial flows that derive from it," the FATF said.

Anti-money laundering and counter-terrorist financing (AML/CTF) controls are becoming more effective at identifying HT offences. The study details numerous case studies where tight typologies have resulted in financial intelligence reports that helped to identify HT syndicates.

The researchers also looked in detail at 28 national AML/CFT risk assessments. Of these, only 14 specifically mentioned human trafficking as a money laundering risk, while none identified human trafficking as a terrorist financing risk.

"They provided little information on the financial flows or the laundering of the proceeds of human trafficking," the report said. "As a predicate crime to money laundering, the financial flows from human trafficking can differ significantly from one case to another."

The FATF said there was a need for far greater focus in this area from national regulators, financial intelligence units and reporting entities.

"Globally, there has not been sufficient focus on how to use financial information to detect, disrupt and dismantle human trafficking networks," it said.

ABOUT THE AUTHORS

TROND VAGEN, Asia Editor, Thomson Reuters

Trond Vagen is the Asia editor for Thomson Reuters Regulatory Intelligence, based in Singapore. He joined Thomson Reuters with the 2010 acquisition of Complinet, which he had been with since early 2008. Trond has covered regulatory compliance issues in Asia and Europe since 2004. He has previously worked for The Deal, Standard & Poor's and Compliance Online, covering issues spanning from M&A deals and private equity in Asia to reporting on EU stock markets.

PATRICIA LEE, Chief Correspondent, Banking and Securities Regulation, Asia, Thomson Reuters

Patricia Lee is Chief Correspondent, banking and securities regulation, Asia for Thomson Reuters Regulatory Intelligence, based in Singapore. She has broad industry experience spanning banking and finance, commodities, broadcast technology, TV/film production and post-production. Patricia began her career in financial journalism at Thomson IFR Asia where she spent five years reporting on the syndicated loan markets of Southeast Asia and Taiwan. This was followed by a two-year stint in financial book publishing. She has worked as a freelance writer, contributing to international trade publications such as Accounting and Business, TheWealthNet.com, Asian Investor and Variety. Patricia has a B.A. from the National University of Singapore. She is bilingual in Chinese and English and speaks Japanese.

NATHAN LYNCH, Regional Bureau Chief, APAC, Financial Crime & Risk, Thomson Reuters

Nathan Lynch is the head regulatory analyst for Thomson Reuters Governance, Risk and Compliance operations in the Asia-Pacific region. Nathan joined Thomson Reuters's London office in 2000. He returned to Australia in 2002 and has written about regulatory affairs, anti-money laundering and compliance developments for Thomson Reuters' Compliance Complete service across the Asia-Pacific region ever since.

Nathan is a member of the Australasian Compliance Institute and has presented workshops at the ACI's annual governance, risk and compliance conference. Nathan also appears regularly in print and electronic media as a specialist commentator on financial markets and regulation.

NIALL COBURN, Senior Regulatory Intelligence Expert, Thomson Reuters

Niall Coburn is the regulatory intelligence expert for the Asia Pacific region. He joined Thomson Reuters in 2013 from FTI Consulting where he was a Managing Director for regulatory investigations in Australia. Prior to that position, Niall was a Senior Specialist Adviser to the Australian Securities & Investments Commission (ASIC) and Director of Enforcement for the Dubai Financial Services Authority (DFSA). He was part of an international team that wrote the regulatory and financial market laws and rules for the Dubai International Financial Centre.

Niall is a Barrister of the High Court of Australia and holds a Bachelor of Arts (Economics) and Law degrees from University of Tasmania, a Masters of Law degree from Melbourne University and a Diploma of Business Administration from Mt Eliza Business School. Niall has over twenty years experience in financial markets and international regulation. In 2002, he was awarded an ASIC Australia Day Honour Medal for his work in corporate investigations.

Niall began his career as a legal aid lawyer and also worked with Aboriginal legal aid. Upon entering the Victorian Bar in 1987, he specialised in corporate law. He joined ASIC as a Principal lawyer and was involved in a number of high profile corporate investigations in Australia and internationally resulting in convictions. He has worked in the Middle East and Asia liaising with other international regulatory bodies and government agencies.

Niall has published extensively on compliance and financial regulation internationally. He has written a book on corporate investigations and insolvent trading published by Thomson Reuters, and has been a commentator in the Australian Financial Review on financial regulation and compliance.


With a new regulatory alert issued every 7 minutes, how do I ensure compliance?
The answer is Thomson Reuters Regulatory Intelligence
Thomson Reuters Regulatory Intelligence is a single solution that empowers you to make well-informed decisions to confidently manage regulatory risk, while providing the tools to make proactive decisions and action change within your organization.
Learn more at risk.tr.com
The intelligence, technology and human expertise you need to find trusted answers.
the answer company™
THOMSON REUTERS®
© 2018 Thomson Reuters S066967/5-18

RISK MANAGEMENT SOLUTIONS FROM THOMSON REUTERS
Risk Management Solutions bring together trusted regulatory, customer and pricing data, intuitive software and expert insight and services – an unrivaled combination in the industry that empowers professionals and enterprises to confidently anticipate and act on risks –and make smarter decisions that accelerate business performance.

For more information, contact your representative or visit us online at risk.thomsonreuters.com