Monday, May 7, 2018

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week’s agenda, and what is next

Dear members and friends,

I have just read that “British psychologists found that young adults use their smartphones roughly one-third of their total waking hours.” Could you ever see that as an opportunity?

Well, I was surprised with the next sentence in the presentation: “Simply put, all of us can now do banking anytime, anywhere. And many segments of our populations are increasingly comfortable going digital, be it for banking, or to purchase goods and services.”

Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore, can see some benefits in the behaviour of young adults. I don’t know if this is positive thinking, optimism (a mental attitude that interprets situations and events as being optimized), or realism.

Actuaries that have not incorporated in their models that “young adults use their smartphones roughly one-third of their total waking hours” must not feel very well now. Ong Chong Tee cannot help, actuaries have a good dose of pessimism and believe in statistics, not monetary authorities.

{Question to an actuary: How many actuaries does it take to change a light bulb? Answer from the actuary: How many did it take the previous five years?}

Ong Chong Tee’s presentation continues with some interesting developments, like the UK bank that leverages totally on blockchain and biometrics to provide peer-to-peer financial services with the slogan of "everyone is a bank".
We read: “Open Banking broadly captures the concept that a consumer owns information about himself and should be able to share that information with any third party if he chooses, for example through APIs, and to transfer his money to any third party seamlessly.

The effect is to give consumers ownership over their financial data, to make that data portable, and therefore enables switching and choice among financial service providers. This should promote competition to improve pricing and service quality.”

John McAfee has said that our mobile phones have become the greatest spy on the planet. I am sure this is not positive thinking.

James Comey, who has served as the director of the FBI, has said: “Technology has forever changed the world we live in. We’re online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.” I am sure he had a different perspective from Ong Chong Tee.

But it is also true that in Singapore they care about cyber security. We read later in the same presentation: “Recently, we have created an enhanced role of a Chief Cybersecurity Officer as well as appointed a new Chief Data Officer.”

Read more at number 7 below. Welcome to the Top 10 list.

Best Regards,

George Lekatis
President of the IARCP
General Manager, Compliance LLC
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828
The Basel Committee urges full, timely and consistent implementation of Basel III post-crisis reforms

The Basel Committee on Banking Supervision (BCBS) has issued the Fourteenth progress report on adoption of the Basel regulatory framework.

The report sets out the adoption status of Basel III standards for each BCBS member jurisdiction as of end-March 2018.

Introductory statement - IIF International Capital Markets and Emerging Markets Roundtable
Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the IIF International Capital Markets and Emerging Markets Roundtable, Washington DC.

“Ever since the groundbreaking work of Solow in the fifties most policy makers and members of academia - especially in the advanced economies - have inclined to favour free capital flows. Many crises later, the view has somewhat shifted, in particular, regarding emerging markets and developing countries, which is the group of countries that I will focus my remarks on.”

EIOPA defines its supervisory convergence priorities
- The supervisory convergence plan focuses on the implementation of Solvency II and conduct of business supervision.

- EIOPA defined three priority areas, namely the implementation of the common supervisory culture, addressing the risks to the internal market and to the level playing field which may lead to supervisory arbitrage as well as the supervision of emerging risks.

**Number 4 (Page 17)**

Cost of ransomware attack on Atlanta
*The city did not pay the ransom demand.*

New reports indicate the city spent in the region of $2.66m responding to the attack.

Costs included incident response, recovery and crisis management, but the city did not pay the ransom demand, reported to be approximately $55,000.

**Number 5 (Page 18)**

NSA declassified document
VENONA - The U.S. Army’s Signal Intelligence Service, the precursor to the National Security Agency, began a secret program in February 1943 later codenamed VENONA.

The mission of this small program was to examine and exploit Soviet diplomatic communications but after the program began, the message traffic included espionage efforts as well.

**Number 6 (Page 20)**

Iran and India ban cryptocurrencies
Iran’s central bank has banned Iranian banks, credit institutions and currency exchanges from selling or purchasing digital currencies. It says cryptocurrencies, like Bitcoin, are used in money-laundering and financing terrorism, and that they are inherently unreliable and risky.

Iran’s actions follow similar decisions by other central banks, such as the Reserve Bank of India’s decision in April to serve three months’ notice for entities they regulate to cease dealing in digital currencies.

**Number 7 (Page 21)**

**The future of banking - evolution, revolution or a big bang**

Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore, at the German-Singaporean Financial Forum, Singapore.

“The close partnerships at both government and business levels underscore the many common values and strategic interests that we share. For example, in the area of financial services, there is strong emphasis on financial institutions having high standards of conduct and prudence given the importance of savings and investment in our societies.”

**Number 8 (Page 28)**

**The fintech phenomenon - five emerging habits that may influence effective fintech regulation**

Opening remarks by Mr François Groepe, Deputy Governor of the South African Reserve Bank, at the Inaugural Intergovernmental Fintech Outreach Workshop, Council for Scientific and Industrial Research, Pretoria.
“Let us begin with the words of Joseph Schumpeter: “Situations emerge in the process of creative destruction in which many firms may have to perish that nevertheless would be able to live on vigorously and usefully if they could weather a particular storm.” There is no doubt that we are witnessing a wave of disruptive innovation and technology that one can liken to Schumpeter’s ‘creative destruction’, one that will leave no aspect of human endeavour untouched.”

Number 9 (Page 30)

The European Supervisory Authorities EBA, EIOPA, and ESMA (ESAs) conclude a multilateral Memorandum of Understanding with the EFTA Surveillance Authority

The European Supervisory Authorities (EBA, EIOPA, and ESMA - the ESAs) have concluded a multilateral Memorandum of Understanding (MoU) on cooperation, information exchange and consultation with the EFTA Surveillance Authority.

Number 10 (Page 32)

NIST Issues First Call for ‘Lightweight Cryptography’ to Protect Small Electronics

Cryptography experts at the National Institute of Standards and Technology (NIST) are kicking off an effort to protect the data created by innumerable tiny networked devices such as those in the “internet of things” (IoT), which will need a new class of cryptographic defenses against cyberattacks.

Creating these defenses is the goal of NIST’s lightweight cryptography initiative, which aims to develop cryptographic algorithm standards that can work within the confines of a simple electronic device.
The Basel Committee urges full, timely and consistent implementation of Basel III post-crisis reforms

The Basel Committee on Banking Supervision (BCBS) has issued the Fourteenth progress report on adoption of the Basel regulatory framework.

The report sets out the adoption status of Basel III standards for each BCBS member jurisdiction as of end-March 2018.

It includes for the first time the finalised Basel III post-crisis reforms published by the Committee in December 2017. These recent reforms will take effect from 1 January 2022.

As noted by the Committee’s oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS), the Committee expects full, timely and consistent implementation of Basel III post-crisis reforms by member jurisdictions.

Since the last report published in October 2017, member jurisdictions have made further progress in implementing standards. Notably, the report shows that:

- the leverage ratio, based on the existing exposure definition, is now in force in most member jurisdictions

- 24 member jurisdictions have issued draft or final rules for the Net Stable Funding Ratio (NSFR)

- 19 member jurisdictions have issued draft of final rules for the revised securitisation framework

However, the report also shows that:

- limited progress has been made in the implementation of some technical standards whose implementation deadlines passed in 2017. These include the standardised approach for measuring counterparty credit risk exposures, and the capital requirements for bank exposures to central counterparties and for equity investments in funds.
- member jurisdictions continue to work towards implementing Basel III standards that have an implementation deadline within the next 12 months. These include the supervisory framework for measuring and controlling large exposures (LEX), the standard for interest rate risk in the banking book (IRRBB) and the requirements for total loss-absorbing capacity (TLAC).

The Committee urges member jurisdictions to strive for full, timely and consistent implementation of Basel III post-crisis reforms, and will keep monitoring closely the implementation of these reforms.

Fourteenth progress report on adoption of the Basel regulatory framework, April 2018

This report sets out the adoption status of Basel III standards for each Basel Committee on Banking Supervision (BCBS) member jurisdiction as of end-March 2018.
It updates the Committee’s previous progress reports, which have been published on a semiannual basis since October 2011.

In 2012, the Committee started the Regulatory Consistency Assessment Programme (RCAP) to monitor progress in introducing domestic regulations, assessing their consistency and analyzing regulatory outcomes.

As part of this programme, the Committee periodically monitors the adoption of Basel standards.

The monitoring initially focused on the Basel III risk-based capital requirements, and has since expanded to cover all Basel III standards.

These include the finalised Basel III post-crisis reforms published by the Committee in December 2017, which will take effect from 1 January 2022 and will be phased in over five years.

The Group of Central Bank Governors and Heads of Supervision, the oversight body of the Committee, reaffirmed its expectation of full, timely and consistent implementation of all elements of this package.

As of end-March 2018, all 27 member jurisdictions have risk-based capital rules, liquidity coverage ratio (LCR) regulations and capital conservation buffers in force.

Twenty-six member jurisdictions have also final rules in force for the countercyclical capital buffers and domestic systemically important bank (D-SIB) requirements.

With regard to the global systemically important bank (G-SIB) requirements, all members that are home jurisdictions to G-SIBs have final rules in force.

Since the last report published in October 2017, member jurisdictions have made further progress in implementing standards whose implementation deadlines passed at the start of 2018.

These include, notably, the leverage ratio based on the existing (2014) exposure definition, which is now in force in most member jurisdictions.

Also, 24 member jurisdictions have issued draft or final rules for the Net Stable Funding Ratio (NSFR) and 19 member jurisdictions have issued draft of final rules for the revised securitisation framework.
However, rules for these standards are yet to be finalised and come into force in many member jurisdictions.

Limited progress has been made in the implementation of some standards whose implementation deadlines passed in 2017.

These include, notably, the standardised approach for measuring counterparty credit risk exposures (SA-CCR), the capital requirements for bank exposures to central counterparties (CCPs) and for equity investments in funds.

Also, member jurisdictions continue to strive to implement other Basel III standards whose implementation deadline is within a year.

These include the supervisory framework for measuring and controlling large exposures (LEX), the standard for interest rate risk in the banking book (IRRBB) and the requirements for total loss-absorbing capacity (TLAC).

To read more:
https://www.bis.org/bcbs/publ/d440.pdf
Introductory statement - IIF International Capital Markets and Emerging Markets Roundtable

Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the IIF International Capital Markets and Emerging Markets Roundtable, Washington DC.

Ladies and gentlemen,

Ever since the ground-breaking work of Solow in the fifties most policy makers and members of academia - especially in the advanced economies - have inclined to favour free capital flows.

Many crises later, the view has somewhat shifted, in particular, regarding emerging markets and developing countries, which is the group of countries that I will focus my remarks on.

Not only can capital flow reversals and in the extreme form sudden stops create significant costs in terms of output losses, financial instability and even political instability. But from all we know today it is surprisingly difficult to find empirical evidence of capital account liberalization being beneficial in terms of output gains, investment, productivity gains, or risk sharing for countries that have not progressed sufficiently far in their institutional development.

Much of the work on this has been carried out by the IMF and indeed by Maurice Obstfeld himself, so Maurice should correct me if I am wrong, but essentially liberalized capital flows should go hand in hand with functioning judicial systems including well enforced property rights, developed and well regulated financial systems as well as stability-oriented macroeconomic policies. There are even longer lists, but these seem to be the minimum requirements.

So, given that these conditions are not always met fully, should countries resort to capital flow measures if faced with volatile flows?
By the way, I am using the IMF terminology of capital flow measures. These are basically **capital controls plus those macroprudential** measures that aim to limit financial stability risks arising from cross-border capital flows.

I think we all agree that sound domestic policies should always be the first line of defence and that capital flow measures should not substitute for warranted macroeconomic or exchange rate adjustments.

But it is also useful to state an obvious but often overlooked fact: Unlike restrictions on the current account, **the imposition of capital flow measures is not under the jurisdiction of the IMF**, thus, any country can basically adopt such controls as it deems necessary to regulate capital movements. However, capital flow policies are part of the Funds surveillance and as such open to an assessment of their impact on the International Monetary System.

Objectives of capital flow measures usually are to maintain monetary independence, to mitigate exchange rate pressures and to safeguard financial stability. However, **capital controls also come with a cost**, like impairments of financial markets and possible reductions of economic growth due to their distortions.

Evidence on the effectiveness of capital flow measures is mixed, or in the words of Olivier Blanchard: "still surprisingly inconclusive". Work on macroprudential measures has only begun in earnest after 2009, thus, the knowledge about these policies is still limited.

Significant results have been found on the composition of capital flows. There is evidence that they can lower banking inflows and portfolio inflows. But there is no significant evidence for a clear impact on net or gross flows. While there is solid evidence that capital flow measures help countries to conduct an independent monetary policy, there seems to be little or no effect of capital flow measures on the exchange rate.

Although the literature on the impact on financial stability is relatively young, capital flow measures have been found to lower credit growth and to curb bank leverage.

Where does that leave policy makers? There is still a lot we do not know. It seems capital flow measures can help a country to deal with volatile capital flows and reduce the likelihood of a financial crisis. But of course one has to consider the costs and distortions.

I think the Institutional View of the IMF has got it mostly right. To safeguard financial stability countries should be able to use all tools at their
disposal, depending on which are best suited to the task, but as non-distortionary as possible and not as an excuse to shirk difficult decisions on macroeconomic policy.

Given that capital movements are not comparable to trade in real goods and given the diversity of its membership, I see no value in extending the IMF's mandate beyond the existing arrangements regarding capital flows. This would necessitate also a change of the IMF's Articles of Agreement, which could be opening a can of worms.
EIOPA defines its supervisory convergence priorities

- The supervisory convergence plan focuses on the implementation of Solvency II and conduct of business supervision.
- EIOPA defined three priority areas, namely the implementation of the common supervisory culture, addressing the risks to the internal market and to the level playing field which may lead to supervisory arbitrage as well as the supervision of emerging risks.

The European Insurance and Occupational Pensions Authority (EIOPA) published its supervisory convergence plan for 2018-2019 for the insurance sector, focusing on the implementation of Solvency II and conduct of business supervision.

Supervisory convergence should ensure a high, effective and consistent level of supervision throughout the European Union, granting a similar level of protection to all European policyholders and beneficiaries.

To strengthen further supervisory convergence for 2018 and 2019, EIOPA defined the following three priority areas:

1. Implementation of the common supervisory culture and new supervisory tools.
2. Risks to the internal market and the level playing field which may lead to supervisory arbitrage.

The implementation of a common supervisory culture will include the further specification of each of the key characteristics of the common supervisory culture.

In addition, EIOPA will develop common benchmarks for the supervision of internal models, work on a common basis for the supervisory assessment of conduct risks throughout a product’s life cycle, perform a thematic review on travel insurance and define good practices for the supervision of intra-group transactions and risks concentrations.
To address risks to the internal market and to the level playing field, EIOPA will analyse the consistency of the calculations of technical provisions in general and in a cross-border context in particular for non-life business such as the “decennial liability insurance” and “medical malpractice insurance”.

Furthermore, special attention will be paid to the assessment of internal model outcomes, the detection of potential unsustainable cross-border business models and the establishment of specific collaboration platforms where needed.

In the area of supervision of emerging risks, EIOPA will develop good practices on the supervision of IT security and governance, including supervisory expectations on insurance undertakings’ practices on cyber security and explore efficient ways to perform a cyber-attack penetration test.

A thematic review of the insurance industry’s use of big data as well as the monitoring of the potential consequences of the withdrawal of the United Kingdom from the European Union will continue to ensure consistency in supervisory approaches.

The priorities of the supervisory plan were identified according to their impact on policyholders and on financial stability as well as on the level playing field or the functioning of the internal market.

The priority areas include also those areas of supervision where practices across the European Union still differ substantially.

At the beginning of 2019, the supervisory convergence plan will be updated and include a progress report.

On conduct of business supervision, EIOPA has developed a broader strategy to address supervisory convergence from the conduct perspective.

The strategy underlines tools for improving market monitoring and risk identification and mitigation as well as developing proactive supervisory capacities across the European Union with the aim to tackle better potential consumer detriment.

Gabriel Bernardino, Chairman of EIOPA, said: “Achieving supervisory convergence, one of EIOPA’s strategic goals, requires a collective effort by all national supervisory authorities and EIOPA. This supervisory convergence plan sets key priority areas, which are crucial for achieving
high-quality and effective supervision and the implementation of a common supervisory culture across the European Union in the interest of the policy holders.”
Cost of ransomware attack on Atlanta
The city did not pay the ransom demand.

As reported in the Weekly Threat Report of 6 April 2018, the US city of Atlanta recently fell victim to an attack by the SamSam ransomware, which exploits a vulnerability in Java servers.

New reports indicate the city spent in the region of $2.66m responding to the attack.

Costs included incident response, recovery and crisis management, but the city did not pay the ransom demand, reported to be approximately $55,000.

There was also a broader cost in terms of the disruption the attack brought to city-wide services, with residents unable to pay bills and parking tickets as the city’s self-service portal was taken offline.

This case highlights the costs to organisations of ransomware attacks. However, paying a ransom does not guarantee that data will be returned and access to files restored. Nor does paying a ransom prevent a future attack; indeed, it may encourage further attacks.

Investment in cyber security can reduce the likelihood of malware infection and prevent the need for costly clean-up operations.
VENONA - The U.S. Army's Signal Intelligence Service, the precursor to the National Security Agency, began a secret program in February 1943 later codenamed VENONA.

The mission of this small program was to examine and exploit Soviet diplomatic communications but after the program began, the message traffic included espionage efforts as well.

Further analysis showed that each one of the five systems was used exclusively by one of the following subscribers (listed in descending order according to the volume of message traffic which had been collected):

1. trade representatives – Lend-Lease, AMTORG, and the Soviet Government Purchasing Commission

2. diplomats – i.e., members of the diplomatic corps in the conduct of legitimate Soviet embassy and consular business

3. KGB – the Soviet espionage agency, headquarters in Moscow and residencies (stations) abroad

4. GRU – the Soviet Army General Staff Intelligence Directorate and attachés abroad

5. GRU-Naval – Soviet Naval Intelligence Staff

Although it took almost two years before American cryptologists were able to break the KGB encryption, the information gained through these
transactions provided U.S. leadership insight into Soviet intentions and treasonous activities of government employees until the program was canceled in 1980.

The VENONA files are most famous for exposing Julius (code named LIBERAL) and Ethel Rosenberg and help give indisputable evidence of their involvement with the Soviet spy ring.

The first of six public releases of translated VENONA messages was made in July 1995 and included 49 messages about the Soviets' efforts to gain information on the U.S. atomic bomb research and the Manhattan Project. Over the course of five more releases, all of the approximately 3,000 VENONA translations were made public.

To read more:
https://www.nsa.gov/news-features/declassified-documents/venona/

Note from the NSA:
“As NSA/CSS reviews records under the Freedom of Information Act or Mandatory Declassification Review provisions of Executive Order 13526, we will make the material available to the public via the NSA.gov website on the Internet. In addition, NSA/CSS periodically conducts "Special Topical Reviews" of categories of records, such as the Gulf of Tonkin, USS Liberty, UKUSA, and posts those records to this site. Lastly, in accordance with the federal Open Government initiative, we will identify subjects and records for which there is a general public interest. We will meet transparency goals by reviewing those records and including them on this web page.”
Iran and India ban cryptocurrencies

Iran’s central bank has banned Iranian banks, credit institutions and currency exchanges from selling or purchasing digital currencies. It says cryptocurrencies, like Bitcoin, are used in money-laundering and financing terrorism, and that they are inherently unreliable and risky.

The same concerns are expressed widely around the world, including by the Chief of the International Monetary Fund, but many also believe digital currencies and the technology behind them could have a positive effect as a low-cost payment method.

Iran’s actions follow similar decisions by other central banks, such as the Reserve Bank of India’s decision in April to serve three months’ notice for entities they regulate to cease dealing in digital currencies.

The central bank decisions have been concerning for digital currency users in these countries (reportedly around five million in India), but it is too early to say whether these actions will last, have any long-term impact on the wider cryptocurrency market or whether other countries will follow suit.

Some countries are debating the regulation of digital currencies: Japan has recently created a regulatory body for its cryptocurrency exchanges, for example, and others have considered creating their own state-backed digital currencies.

The future of digital currencies is still unknown, which is a major contributing factor to their price volatility, but they are likely to be with us for the foreseeable future.
The future of banking - evolution, revolution or a big bang

Ong Chong Tee, Deputy Managing Director (Financial Supervision) of the Monetary Authority of Singapore, at the German-Singaporean Financial Forum, Singapore.

Dr Johannes Beermann, Member of the Executive Board of the Deutsche Bundesbank, His Excellency Dr Ulrich Sante, Ambassador of the Federal Republic of Germany, Dr Claus Trenner, President of the Singaporean-German Chamber of Industry and Commerce, Distinguished Guests, Ladies and Gentlemen

It is my pleasure to join you this morning at the inaugural German-Singaporean Financial Forum.

Bilateral relations

Singapore and Germany have strong bilateral relations at many levels.

(a) Last year, Chancellor Angela Merkel and Prime Minister Lee Hsien Loong met in Berlin in July, and later, President Halimah Yacob hosted President Frank-Walter Steinmeier during his state visit in November.

(b) Singapore was also invited to the G20 meetings in 2017 during Germany’s Presidency.

The close partnerships at both government and business levels underscore the many common values and strategic interests that we share. For example, in the area of financial services, there is strong emphasis on financial institutions having high standards of conduct and prudence given the importance of savings and investment in our societies.

MAS and our German counterparts, the Bundesbank and BaFin, participate in many international forums and standard-setting bodies including the Financial Stability Board, the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors, and the International Organisation of Securities Commission.
On many issues, we share common interests and positions. In 2010, MAS and Bundesbank established a cross-border collateral arrangement to enhance liquidity provision by widening the pool of eligible collateral for banks.

MAS has a Supervisory Memorandum of Understanding (MOU) with BaFin that provides for mutual assistance and sharing of supervisory information in banking and insurance.

MAS also participates in the annual Deutsche Bank Supervisory College for non-EU regulators and we are pleased to have hosted the most recent one last November.

Given that financial activities are often cross-border in nature, such international co-operation will be of increasing importance, including to facilitate innovative services as well as to mitigate the risks that some these may present.

It is also in this spirit that I congratulate the establishment of this partnership forum. It is an excellent example of a co-operation platform that allows our industry players to engage one another in open discussions, to identify common challenges and working opportunities.

This forum also provides for perspectives from government, central bank, regulator and academia.

**Future of banking**

Allow me now to share some thoughts on the conference theme around the future of banking.

This is clearly a topical subject in the face of the ongoing Technology Revolution around us.

Many of us will probably have heard of the famous quote by Bill Gates, that "people do not need banks, they need banking".

In other words, with the rise of new FinTech players, activities that are considered banking services need not be provided by traditional banks alone.

Technology or e-commerce giants like Alibaba and Tencent have moved into the financial services space, as they seek to strengthen their customer-centric propositions and services.
Business disruptions need not be led only by the large firms. Smaller nimble start-ups have also sought to un-bundle the banking value chain by focusing on niche areas such as financial advisory services and consumer finance.

There are two underlying factors:

(a) One, is the arrival of the smartphones that launched a new era of mobile apps. Banking has moved from physical branches, to the desks, and now to the palm.

Recently, I read a report that British psychologists found that young adults use their smartphones roughly one-third of their total waking hours.

Simply put, all of us can now do banking anytime, anywhere. And many segments of our populations are increasingly comfortable going digital, be it for banking, or to purchase goods and services.

(b) Second, the accessibility afforded by technology has led banks to shift away from a production-consumption model. Traditional banking models are based on making available the range of the services that a customer need.

Today, competition centres on the customer experience. One of our local Singapore banks has a tag line on making banking joyful. The notion of delighting a customer opens up a whole field of competitive ideas as to how to generate that positive experience. This is what the FinTech players have sought to do, and this is what banks are fighting back on. Banks will have the advantage of being highly regulated and trusted, that smaller and newer players may find it hard to challenge.

The general consensus is that many FinTechs and the established financial institutions will collaborate.

There is a natural synergy here:

(a) Collaboration with financial institutions enables FinTech players and technology firms to broaden their reach.

(b) On the flip side, FinTech solutions present established financial institutions with opportunities to enhance their product offerings or to improve operational productivity.
McKinsey estimated that enhancing digital capacity and adopting technologies could result in productivity gains worth roughly US$350 billion for the global banking industry by 2025.

But the competition will remain intense. Large internet-based firms with their massive customer base can be serious contenders for customer mind-share and wallets including in the area of financial services.

There is another development that has gained traction. We see the emergence of fully digital banks that operate entirely online with no physical branches, but are able to provide similar services as the traditional brick-and-mortar banks.

Fidor Bank, founded in Germany, is one such example. WeBank in China is another.

DBS' Digibank, a mobile-only bank in India, is also completely branchless and in less than two years, have signed up more than 1.5 million customers. All three have different origins and operate very different business models. I am sure the panellists later will discuss these further when they talk about the future of banking.

Let me turn to this forum’s theme question on whether we will witness an evolution or revolution in banking. I believe it will be both. A lot of attention and excitement have been created by services going digital.

This digitisation of services have transformed the customer experience say for on-boarding or transactional purposes; but frankly, are not ground-breaking in themselves.

As one commentary noted, this is no different from reading an actual newspaper or reading the news online. But a revolution is also happening when new digital services or business models emerge that employ say, artificial intelligence (AI) or blockchain technologies. These can fundamentally change how we borrow, save, pay, invest or insure.

As an example, there is a UK bank BABB that leverages totally on blockchain and biometrics to provide peer-to-peer financial services with the slogan of "everyone is a bank". Time will determine the winners and losers as this cycle of technology disruption takes it course.

Open banking

Open Banking broadly captures the concept that a consumer owns information about himself, and should be able to share that information
with any third party if he chooses, for example through APIs, and to transfer his money to any third party seamlessly.

The effect is to give consumers ownership over their financial data, to make that data portable, and therefore enables switching and choice among financial service providers. This should promote competition to improve pricing and service quality.

The EU has started on this journey by making payment and data interconnectivity between banks and non-banks mandatory, through the Payment Services Directive 2.

Australia has also announced that it will legislate a national Consumer Data Right in 2018, allowing consumers open access to all their data including banking-related ones.

While these hold a lot of promise by promoting consumer interests and welfare, there are other details to consider. For example, what primary data rightfully belongs to the customer, and what about secondary data about the customer that a bank had made sense of? How should a customer's data be packaged for onward sharing? How do we develop technical standards to share this information efficiently and securely? Who should pay for these?

In Singapore, we subscribe to the notion of banks sharing their data openly as a larger good. Some of the operational details have to be worked out. In MAS' engagement with the banking industry, there is broad consensus as to the benefits of open banking.

What we see is an opening up of customer data as a ground-up process led by the banks themselves. We believe this is a constructive development, that industry players themselves see the value in doing so.

Role of financial regulators

In my remarks so far, it should be obvious that financial regulators will have active roles in the business and technology transformation in the banking industry.

Regulators need to have a sharp understanding of emerging technologies and new business models, and to be alert to potential risks. Only then are we able to exercise thoughtful judgment.

There will be a balance between supporting innovation and technology use, while pre-empting new or heightened risks that these may present.
MAS takes an even-handed approach by providing a regulatory regime that is risk-proportionate across the range of institutions involved in regulated financial activities.

We seek to provide the environment, and even to encourage new FinTech and other players to establish themselves to compete, collaborate and innovate.

We allow for adoption of technology and innovation in financial services, especially those that hold promise in raising efficiency, in creating new opportunities, in enabling new or value-adding services or simply to manage risks better.

MAS adopts a "materiality and proportionality" test, and seeks to right-size regulations to be fit-for-purpose; for both traditional as well as new business models, according to the risks the activity poses.

For example, in the new Payment Services Bill that MAS has consulted on, regulatory requirements for payment activities will be differentiated according to the risks that specific activities pose rather than apply a uniform set of regulations on all payment service providers.

Regulation comes in when the risk posed becomes material or crosses a threshold. The weight of regulation must be proportionate to that risk. Singapore is one of the first jurisdictions to have established regulatory sandboxes where firms can experiment their innovative solutions in a contained environment, with access to a limited pool of actual customers.

What we will diligently protect is the trust and credibility in our financial system. We will also be paying closer attention to financial institutions' management of cyber-threats and to new forms of financial stability vulnerabilities as digitisation blurs the boundaries across geography and industries.

Recently, we have created an enhanced role of a Chief Cybersecurity Officer as well as appointed a new Chief Data Officer. I believe there is much we can share and learn from other central banks, financial regulators and even law enforcement agencies, such as our European counterparts.

Looking ahead

Finally, there are other areas that should matter to all of us amidst the ongoing transformations in the banking industry.
One is the important issue of financial inclusion. In the quest to innovate and as banks develop the sophistication to sharpen the profile of each customer, we should not overlook the need for financial inclusion - especially access to basic banking and financial services for under-served communities.

Another area is in the responsible use of technology tools. Earlier this month, MAS announced the setting up of a regulator-industry grouping to co-create a guide to promote the responsible and ethical use of AI and data analytics by financial institutions.

This Committee is known by its acronym FEAT - which stands for Fairness, Ethics, Accountability and Transparency. This gives you a good idea of its mandate. The key is as technology and data analytics usage become more prevalent, the responsible use of these is equally paramount.

**Conclusion**

To conclude my remarks, allow me to resurrect a quote from a speech by President Kennedy in 1966, which I thought is apt even in current times.

[quote] There is a Chinese curse which says 'May he live in interesting times'. Like it or not we live in interesting times. They are times of danger and uncertainty; but they are also more open to the creative energy of men than any other time in history. [unquote]

Many will agree that we are living in interesting times; and a forum like this will be useful in bringing together the constructive and creative energy of experts like yourselves to share, to understand and to co-operate.

Ultimately, it falls on all of us to do our part to make the future more promising and enriching for this and the generation that follows.

Thank you
Number 8

The fintech phenomenon - five emerging habits that may influence effective fintech regulation

Opening remarks by Mr François Groepe, Deputy Governor of the South African Reserve Bank, at the Inaugural Intergovernmental Fintech Outreach Workshop, Council for Scientific and Industrial Research, Pretoria.

Introduction

Good morning, ladies and gentlemen.

Welcome to the inaugural Intergovernmental Fintech Outreach Workshop.

Let us begin with the words of Joseph Schumpeter: “Situations emerge in the process of creative destruction in which many firms may have to perish that nevertheless would be able to live on vigorously and usefully if they could weather a particular storm.”

There is no doubt that we are witnessing a wave of disruptive innovation and technology that one can liken to Schumpeter’s ‘creative destruction’, one that will leave no aspect of human endeavour untouched.

Financial services in particular are within the eye of the storm of the change as a result of financial technology, or ‘fintech’.

An elementary Google search on fintech results in no fewer than 35.2 million hits.

Investment in fintech over the last three years is estimated to have been well over US$300 billion dollars. Attention to the emergence of fintech has come from every quarter.

There have been contributions from the World Economic Forum reflecting the potential of distributed ledger technology across wide-ranging financial services and activities.
The International Monetary Fund has been vocal about the potential impact of cryptocurrencies. More recently, under the Argentinian presidency, the G20 has committed to deepening the analysis on how financial inclusion could be achieved through digital innovations.

All of these examples suggest a heightened expectation of shifts to financial services as a result of fintech.

At the outset, it may be appropriate to attempt to define what fintech is.

‘Fintech’ usually refers to innovative start-ups or underlying technologies such as blockchain, cloud computing, and machine learning.

Founded on an activity-based analysis conducted by the Financial Stability Board (FSB), the evolving definition of ‘fintech’ is that it is neither the fintech firms, nor the start-ups, nor the emerging technologies.

Rather, ‘fintech’ is the technology-enabled innovation in financial services as a result of the process of ‘creative destruction’. It may lead to new business models and new configurations within financial services.

To read more:
https://www.bis.org/review/r180426e.pdf
The European Supervisory Authorities (EBA, EIOPA, and ESMA - the ESAs) have concluded a multilateral Memorandum of Understanding (MoU) on cooperation, information exchange and consultation with the EFTA Surveillance Authority.

This multilateral MoU establishes practical arrangements between the ESAs and the EFTA Surveillance Authority in relation to the adoption of acts by the EFTA Surveillance Authority on product intervention, breach of European Economic Area law, action in emergency situations, mediation, as well as on the adoption of specific opinions, effective within the EEA-EFTA States.

The EFTA Surveillance Authority has been vested with the powers to adopt decisions and formal opinions addressed to competent authorities and/or financial market participants and financial institutions in the EEA States based on the amended Agreement on the European Economic Area (EEA Agreement) of 30 September 2016.

The EEA Agreement guarantees equal rights and obligations within the Internal Market for individuals and economic operators in the European Economic Area.

It provides for the inclusion of European Union legislation covering the four freedoms — the free movement of goods, services, persons and capital — throughout the 31 European Economic Area States.

EFTA Surveillance Authority monitors compliance with the EEA Agreement in Iceland, Liechtenstein and Norway, enabling those Member States to participate in the Internal Market of the European Union.

It was established by the EEA Agreement, an international agreement which enables the three EFTA States to participate fully in the European internal (or single) market.
The EFTA Surveillance Authority’s role in the EEA-EFTA States mirrors the role of the ESAs in the European Union Member States.

NIST Issues First Call for ‘Lightweight Cryptography’ to Protect Small Electronics

Cryptography experts at the National Institute of Standards and Technology (NIST) are kicking off an effort to protect the data created by innumerable tiny networked devices such as those in the “internet of things” (IoT), which will need a new class of cryptographic defenses against cyberattacks.

Creating these defenses is the goal of NIST’s lightweight cryptography initiative, which aims to develop cryptographic algorithm standards that can work within the confines of a simple electronic device.

Many of the sensors, actuators and other micromachines that will function as eyes, ears and hands in IoT networks will work on scant electrical power and use circuitry far more limited than the chips found in even the simplest cell phone.

Similar small electronics exist in the keyless entry fobs to newer-model cars and the Radio Frequency Identification (RFID) tags used to locate boxes in vast warehouses.

All of these gadgets are inexpensive to make and will fit nearly anywhere, but common encryption methods may demand more electronic resources than they possess.

Today, NIST is launching an effort to create worthy solutions to the problem of securing data in this sort of constrained environment. As an initial step, it seeks assistance in developing requirements and guidelines for these solutions.

The Draft Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process is the first draft of this request, written with the software development community in mind and aimed at ensuring that the formal request—slated for release later this spring—will produce the sort of encryption algorithms that developers agree will help.
The draft document is available now on the NIST website (you may visit https://csrc.nist.gov/Projects/Lightweight-Cryptography). A Federal Register Notice will soon announce a public comment period so that the community can weigh in on the draft submission guidelines.

The ultimate goal is to develop lightweight encryption standards that benefit the entire marketplace. According to NIST computer scientist Kerry McKay, effective standards must bring a well-defined solution that applies to a wide class of situations—and that made the wording of the request tricky.

“The IoT is exploding, but there are tons of devices that have nothing for security,” McKay said. “There’s such a diversity of devices and use cases that it’s hard to nail them all down. There are certain classes of attacks to consider, lots of variations. Our thinking had to be broad for that reason.”

Many of the manufacturers who create these small devices say that the time is right for establishing effective standards.

“As industries adopt authentication apps for things like flu-shot syringes and baby formula, it’s important that there is agreement on security practices,” said Matt Robshaw, a technical fellow at Impinj, a company that develops RAIN RFID technology used to keep track of these kinds of objects. “It’s a good time to begin to establish guidance about which of these techniques will be most appropriate.”

To ensure they were getting off to the right start, McKay and the team members spent four years consulting with industry groups ranging from smart power grid experts to auto manufacturers. Their advice led the team to stipulate that submitted algorithms must have been published previously and been analyzed (though not necessarily adopted) by a third party.

“We feel it’s a fair request because people have been working on crypto for constrained environments for several years now,” McKay said. “We want to see things that the world has looked at already.”

These solutions typically use symmetric cryptography—the less resource-intensive form, in which both the sender and recipient have an advance copy of a digital key that can encrypt and decrypt messages.

The NIST team specifies that these algorithms should provide one useful tool in symmetric crypto applications: authenticated encryption with associated data, or AEAD, which allows a recipient to check the integrity of both the encrypted and unencrypted information in a message.
They also stipulate that if a hash function is used to create a digital fingerprint of the data, the function should share resources with the AEAD to reduce the cost of implementation.

McKay said that while the AEAD and hash tools should cover nearly everything that a developer would want to do with symmetric cryptography, she and the team are looking forward to comments from the public on whether the draft’s requirements are sufficient.

“We will be relying on community feedback to determine what other use cases we should include in subsequent editions of the pub,” she said. “We want the entire lightweight crypto standards development process to be open and transparent, with the public involved at every step.”

After the Federal Register notice appears, NIST will be accepting comments on the draft for 45 days, and will consider these comments before releasing the formal submissions guideline document. Following its release, NIST anticipates a 6-month submission window for lightweight cryptographic algorithms.
Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudice the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudice the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.
International Association of Risk and Compliance Professionals

You can explore what we offer to our members:

1. **Membership** – Become a standard, premium or lifetime member.

   You may visit:  
   [www.risk-compliance-association.com/How_to_become_member.htm](http://www.risk-compliance-association.com/How_to_become_member.htm)

   Become a lifetime member of the association, and to continue your journey without interruption and without renewal worries. You will get a lifetime of benefits as well.

   You can check the benefits at:  
   [www.risk-compliance-association.com/Lifetime_Membership.htm](http://www.risk-compliance-association.com/Lifetime_Membership.htm)

2. **Weekly Updates** - Subscribe to receive every Monday, the Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next:  
   [http://forms.aweber.com/form/02/1254213302.htm](http://forms.aweber.com/form/02/1254213302.htm)

3. **Training and Certification** - The Certified Risk and Compliance Management Professional (CRCMP) training and certification program has become one of the most recognized programs in risk management and compliance.

   There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

   You can find more about the demand for CRCMPs at:  

   For the distance learning programs, you may visit:  
   [www.risk-compliance-association.com/Distance_Learning_and_Certification.htm](http://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm)

   For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements. We tailor presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.
Some CRCMP jobs:


This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience. Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
5. Approved Training and Certification Centers (IARCP-ATCCs) - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor-led CRCMP and CISRCP training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more: www.risk-compliance-association.com/Approved_Centers.html