IDEAS FOR LEADERS | DECEMBER 2018

# banking insight

PP 17327/05/2013(032407)

**CENTS AND SUSTAINABILITY**

A Balancing Act In Trade-Based Money Laundering Compliance

**BIG DATA MEETS BIG BROTHER**

## GLOBAL FINANCIAL CRISIS DECENNIAL

### AT BANKING'S 'TRUE NORTH'?

A decade since the global financial crisis, how much safer are banks today? We review the hits, misses, almost-theres, and future trends.

GREAT TO GOOD

ISSN 2231-8267

A PUBLICATION OF
ASIAN INSTITUTE OF CHARTERED BANKERS

## Editor's Note

# PROFESSIONALISING THE BANKING INDUSTRY

**WITH SEVERAL ISSUES UNDER OUR METAPHORICAL BELT,** this is an opportune time for us at *Banking Insight* to review our goals to ensure that we are seamlessly aligned with our overarching agenda of sharing knowledge and upskilling to professionalise banking talent.

To achieve this, in every issue, we strive to cover the most compelling and relevant developments affecting the industry, adding value by examining these issues within the Malaysian and ASEAN context. This time around, we revisit digital disruption and its impact on banking, because the urgency to embrace technology and innovate business models to deliver greater value is snowballing for financial institutions. In our cover story 'Banking in the Digital Age', we look at how banks are transforming their business models to integrate technologies and deliver better value, by adopting tools such as cloud, analytics and mobile. Looking further ahead, Manish Bahl of Cognizant Technology Solutions, a distinguished speaker at our recent banking conference on Mastering the Application of Digital Thinking and Technology in Banks is urging financial institutions to look beyond the current fintech hotspots of mobile wallets and payments to address the void in slow money, which refers to any future spending or saving by consumers, e.g. pensions, insurance and investments. Meanwhile, EY's Chow Sang Hoe imagines banks as platforms for financial transactions, where consumers and producers interact using smartphones as the universal banking tool. Senior contributing writer Angela Yap, on the other hand, imagines how retail banks can reconfigure their branches – which are still responsible for approximately 30% of a bank's operating costs and 45% of all banking revenue – to become digitally anchored, mobile-centric and more competitive and viable in this shifting landscape. Other issues worth checking out in this issue include a look at the evolving regulatory landscape for bitcoin and cryptocurrencies *vis-à-vis* fiat currencies and an overview of financial inclusion and social finance initiatives.

While it is critical for Malaysian and ASEAN financial institutions to keep abreast and ahead of technological innovation, it is even more imperative that talent is trained and upskilled to integrate technological know-how with impeccable ethics and professional standards. This is a key strategic agenda at the Asian Institute of Chartered Bankers (AICB), which seeks to imbue ethics and elevate professional standards among banking professionals in Malaysia and the region. In this issue, I am sharing at length on ethics, integrity and professionalism, the three pillars of financial stability. As today's banking industry evolves rapidly, driven by regulatory and technology advancements, it needs talent who are not only competent and skilled, but who possess strategic insights and adaptability, underpinned by "ethics, integrity and professionalism to contribute to the stability of the financial industry and the greater economy". I am also proud to share some of AICB's key initiatives that will elevate the industry's professional standards and governance: hard on the heels of our earlier commitments with stakeholders to implement professional standards for the holistic industry and anti-money laundering, with effect from 1 January 2023, reporting submissions by Development Financial Institutions (DFIs) to Bank Negara Malaysia must be undersigned by DFI officers who are qualified Chartered Bankers. This will go further towards raising the profile and relevancy of the Chartered Banker qualification, while ensuring enhanced corporate governance and public trust in the financial ecosystem and market. As AICB matures, we intend to keep upholding our two key roles: as custodian of professional banking standards and membership development. *Banking Insight* is a key tool for promulgating and championing banking professionalism and we hope to keep improving and serving our members and readers better in the years to come. ✱

*Hope you have a fruitful read.*

**The Editor**

**+ This time around, we revisit digital disruption and its impact on banking, because the urgency to embrace technology and innovate business models to deliver greater value is snowballing for financial institutions.**

ASIAN INSTITUTE OF CHARTERED BANKERS

# bankinginsight

Ideas for Leaders




**Editor** | Prasad Padmanaban **Assistant Editor** | Shireen Kandiah
**Writers** | Amrita Kundu, Angela Yap, Stephanie Francesca Pereira, Hisyam Ali, Anirban Kundu, Nazatul Izma

**PUBLISHER**

**Asian Institute of Chartered Bankers** (35880-P)
*(formerly known as Institut Bank-Bank Malaysia)*
Wisma IBI, 5 Jalan Semantan, Damansara Heights, 50490 Kuala Lumpur Malaysia
Tel: +603 2095 6833 Fax: +603 2095 2322 Email: enquires@aicb.org.my

**PUBLISHING CONSULTANT**

**Executive Mode Sdn Bhd** (317453-P)
Tel: +603 7118 3200 Fax: +603 7118 3220 Email: executivemode@executivemode.com.my

**PRINTER**

**Percetakan Lai Sdn Bhd**
No.1, Persiaran 2/118C, Kawasan Perindustrian Desa Tun Razak, Cheras, 56000 Kuala Lumpur
Tel: +603 9173 1111 Fax: +603 9173 1969


**We want to hear what you have to say on Banking Insight.**

Why not drop us a line now? e-mail: **enquires@aicb.org.my** | Visit us online at our website **www.aicb.org.my**

# CONTENTS PAGE
**December 2018**

## BLOCKCHAIN-ONLY BOND

The World Bank launched the first blockchain-only bond with Commonwealth Bank of Australia on 23 August 2018. The pioneering two-year debt instrument named bond-*i* – which formally stands for 'blockchain operated new debt instrument' but is likely also a silent nod to the continent's famous beach – raised AUD110 million with investors drawn from Australian banks and state treasuries. The uptake and range of state investors reflect the market's keen curiosity in distributed ledger technology. Increasingly, the World Bank has been piloting experimental proof-of-concepts out of its blockchain innovation lab launched in June 2017. These pilot projects are aimed at leveraging the use of disruptive technologies to achieve its twin goals of poverty alleviation and enhanced living standards. ✱

In the first six months of 2018, GBP503.4 million was **STOLEN BY CRIMINALS THROUGH AUTHORISED AND UNAUTHORISED FRAUD.** ~ UK Finance, *Fighting Fraud: Helping to Keep Customers Safe.*

## MALAYSIA UPS ANTE ON INCLUSIVE FINANCE

Bank Negara Malaysia, Malaysia Digital Economy Corporation, and the United Nations Capital Development Fund upped the ante on financial inclusion for the nation's middle- and low-income groups with the launch of the Digital Finance Innovation Hub and Inclusive Fintech Accelerator Program. Launched on 26 September 2018, the hub encourages financial institutions and fintech start-ups to innovate and promote financially inclusive technologies to meet the needs of the underserved in Malaysia. Corollary goals include higher economic efficiency in financial intermediation and cost reduction by providing an expanded menu of options, faster provision of financial services as well as more effective utilisation. ✱

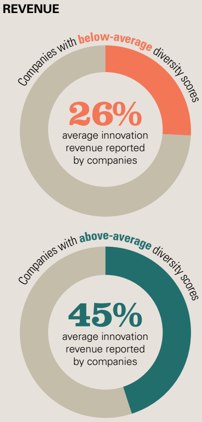

Close to 50% of the adult population in low- and middle-income Asia-Pacific economies **DOES NOT HAVE A BANK ACCOUNT.** ~ IMF, Financial Inclusion in Asia-Pacific.

# Diverse Leadership Boosts Innovation

A Boston Consulting Group study suggests that more diverse leadership teams result in more and better innovation and improved financial performance. Companies with above-average diversity in their senior teams clocked significantly better payoff from innovation revenue – 19 percentage points higher compared to companies with below-average leadership teams – as well as higher EBIT margins.

The global consultancy's article, *How Diverse Leadership Teams Boost Innovation,* explained: "People with different backgrounds and experiences often see the same problem in different ways and come up with different solutions, increasing the odds that one of those solutions will be a hit. In a fast-changing business environment, such responsiveness leaves companies better positioned to adapt." ✱

**EXHIBIT 1 COMPANIES WITH MORE DIVERSE LEADERSHIP TEAMS REPORT HIGHER INNOVATION REVENUE**




**SOURCE** BCG diversity and innovation survey, 2017 (n=1,681)
**NOTE** Average diversity score calculated using the Blau index, a statistical means of combining individual indices into an overall aggregate index

# Unlocking Sustainability's Value

IN THIS EXCLUSIVE INTERVIEW, WE CHECK IN WITH FELLOW CHARTERED BANKER MR LEE LUNG NIEN, CEO OF CITIBANK BERHAD (CITI), FOR HIS VIEWPOINTS AND VISION ON BANKING'S ROAD AHEAD.

**Q As a veteran banker of 27 years, you've experienced the gamut of operations, both local and global, ranging from financial markets sales to anti-money laundering compliance. How significant has the operational landscape changed during this time?**

Change has been revolutionary and transformative with the focus on client-centric financial solutions. Digital technology has been the catalyst for this change and it is about speed in responding to market demands and customer needs and investing in a forward compatible growth strategy that enables us to be the best for our clients.

Also, earning and maintaining the public's trust by constantly adhering to the highest ethical standards has always been a priority. We ask our colleagues to ensure that their decisions are in our clients' interests, create economic value and are always systemically responsible.

When we do these things well, we make a positive financial and social impact in the communities we serve and show what a global financial services leader can do.

Today, Citi's revenue base is well balanced across products and regions. We have multiple engines for client-led growth and are poised to capture opportunities anywhere we see them around the world.

Our Global Consumer Bank operates three businesses – the largest global credit card issuer, a retail bank with an urban footprint and a commercial business serving mid-sized clients with cross-border needs. Focus is on driving growth in the US, Mexico and Asia, attractive markets where our scale and investments position us to capture additional market share as we put digital and mobile at the core of a simpler, better client experience.

Our Institutional Clients Group is scaled to serve multinational companies, emerging market leaders, governments, investors and ultra-high net worth households that rely on our unique global network, insights and local market expertise to meet their banking needs. We serve clients across more than 160 countries and facilitate an average of $4 trillion of flows daily.

We are in a strong place today as we seek out opportunities to help address societal challenges that impact our clients and communities, including job creation and readiness, affordable housing and protecting the environment through sustainable growth. The journey for me has been fulfilling and a great adventure of learning and growing as a leader, of sharing the passion and knowledge gained with our future generation of banking professionals and experts.

**Q This year marks a decade since the Global Financial Crisis. In your estimation, how far along is the industry on the road to greater probity and restoration of public trust?**

Since the last Global Financial Crisis, the banking industry has come a long way in becoming stronger in many ways. Significant regulatory changes have made banks simpler, smaller, safer and stronger. Over the years, the industry has strengthened focus on treating customers fairly via building and also significantly enhanced risk management

capabilities, thereby building strong capital and low non-performing loan levels. Today, we are truly stronger as an industry and this is something that was not achieved in an instant. It calls for strong affirmation of high leadership standards and corporate values. The restoration of public trust is a continuing journey of building relationships that are respected and credibility that is earned.

**Q The Chartered Banker designation, recognised as the gold standard**

Over the years, the industry has strengthened focus on treating customers fairly via building and also significantly enhanced risk management capabilities, thereby building strong capital and low non-performing loan levels. Today, we are truly stronger as an industry and this is something that was not achieved in an instant. It calls for strong affirmation of high leadership standards and corporate values. The restoration of public trust is a continuing journey of building relationships that are respected and credibility that is earned.


**in banking, is designed to create transformative human talent that meets industry needs. What are your expectations of the desired skill set in next-generation talent?**

Our expectations are for banking professionals with a solid understanding of the financial services industry and who will be able to make professional, ethical and well-informed decisions in a demanding work environment.

Given the dynamism and disruption happening in our industry, we seek forward compatible, client-centric talent who can visualise what a better future can look like and who can influence others to work together to create that better future.

**Q 'Profitability vs. Soundness' is the perpetual conundrum faced by industry executives. How can bankers practically navigate these seemingly opposing goals?**

By living out the values and principles we hold fast to consistently in all situations, mindful that present profitability has to be built on a firm foundation that will safeguard the interests of all stakeholders. We need to be true to ourselves and to all whom we have responsibility for. It is about honesty and principled, intentional business leadership.

**Q Every responsibility of the CEO – balancing risk, maintaining growth, deploying capital investments, strengthening investor relations – can be viewed through the lens of sustainability. Few though have been able to translate the benefits of sustainability into clear financial value. What is needed to bridge this gap?**

Companies and leaders the world over share a common purpose when it comes to the area of sustainability and the intrinsic value it generates to secure future economic prosperity. Also, today's millennial workforce has unequivocally expressed their preference for careers in socially responsible companies. Clearly, future growth and economic well-being hinge on the ability of corporations and countries to build sustainable environments, cultures and enterprises.

I would agree that the challenge faced today is of course that of being able to unlock the value of sustainability and the measure of it in terms of clear financial value. Nevertheless, the progress in the development of resilient and robust risk management models, identifying social and environmental impact in a volatile and complex global landscape, the nurturing of talent that are engaged in looking for meaning and purpose beyond profit and a relentless pursuit of innovation to redefine customer experience provide some good benchmarks for evaluating current achievements in sustainability.

Accelerating the progress path will require the courage to perhaps make tough decisions in the present to benefit future economies and our next generation. The question, of course, is our readiness for radical change and our willingness to perhaps sacrifice, make bold moves and the ability to look beyond our own environments.

**Q As we usher in the New Year, what's on your wish list for 2019?**

I would not call it a wish list. We look ahead with optimism anticipating new trajectories of growth aligned to our mission at Citi to serve as a trusted partner to our clients by responsibly providing financial services that enable growth and economic progress.

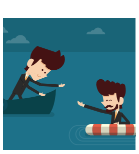
A relentless pursuit of possibilities inspired by innovation, a passion for excellence and to positively impact the lives of the communities we serve.

**+ Companies and leaders the world over share a common purpose when it comes to the area of sustainability and the intrinsic value it generates to secure future economic prosperity.**

# Global Financial Crisis Decennial

## AT BANKING'S 'TRUE NORTH'?

A decade since the global financial crisis, **how much safer are banks today?** We review the hits, misses, almost-there's, and future trends.



**+ The GFC challenged the theory of 'too big to fail', i.e. that the downfall of certain large, highly interconnected financial institutions would be so disastrous to the status quo that they must be supported by government at any cost.**

In 1962, as President John F. Kennedy stood on a podium and announced the winner of a coveted science award, disagreement broke out backstage amongst organisers on how to proceed with the ceremony.

Oblivious that their bickering could be heard over the public announcement system, the president threw a glance over the nervous audience and said drily: "This is the way the administration is really run."

Ten years since the global financial crisis (GFC), time's up for banking to take a leaf out of JFK's book and ask ourselves: "How has this administration really been run?"

Is the financial world any closer to making itself more stable, robust, and ethical?

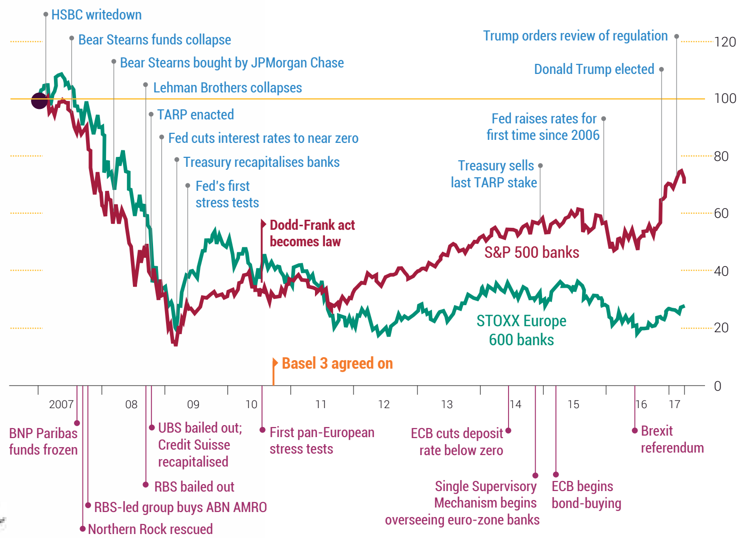
Here's an overview of the big issues – what we did, didn't and have yet to get right – en route to banking's True North.

### TOO BIG TO FAIL

Some survived, some didn't, others grew bigger than before.

The GFC challenged the theory of 'too big to fail', i.e. that the downfall of certain large, highly interconnected

**CHART 1 SHARE PRICES, 1 JANUARY 2007=100**




**SOURCE** 'Thomson Reuters: The Economist

financial institutions would be so disastrous to the status quo that they must be supported by government at any cost. Notable critics include former Federal Reserve Chairman Alan Greenspan, who said, "If they're too big to fail, they're too big"; Nobel prize-winning economists Joseph Stiglitz and Paul Krugman; and the Bank of International Settlements, also known as the 'Central Banks' Central Bank'.

*Financial Times* in *What Happened to the 'Too Big to Fail' Banks?* on 28 August 2017, wrote: "While some have fallen down the global league table, many are larger today…Fears of systemic collapse pushed governments into bailing out hundreds of financial institutions around the world. So it is ironic that the world's biggest banks have got bigger, not smaller, in the decade since."

Although US-based banks such as Lehman Brothers no longer exist and global names like Citibank have shrunk by total assets, other American stalwarts such as JPMorgan Chase and Bank of America (BoA) are larger today on the back of mergers and acquisitions of its troubled rivals. In 2008, JPMorgan Chase acquired both Bear Stearns and Washington Mutual, and BoA wrested control of Merrill Lynch.

This stands in stark contrast to most European banks, with the exception of Deutsche Bank, which are significantly smaller today in terms of total assets and lag their American counterparts in revamping the way they do business.

Zooming its way to the top of the league table is a 'new kid on the block'. China's banks have made an indelible impression with four frontrunners – Industrial and Commercial Bank of China, China Construction Bank, Agricultural Bank of China and Bank of China – now among the world's top four with a combined US$13.637 trillion in total assets.

In totality, it would seem that post-crisis reforms have yet to fully resolve 'too big to fail'. For these institutions, government support or subsidy is most likely implicit in their growth.

## REINING IN EXCESSIVE RISK

When the bubble burst, banks were immediately perceived to be high risk and investors were more risk averse. Such heightened or alarmist sentiments have waned…but is it warranted?

For insight into this, we refer to Marisa Basten and Antonio Sánchez Serrano's April 2018 case study, *European Banks After the Global Financial Crisis: A New Landscape,* of 32 Europe-based banks as an indicator of the overall realities of banking.

The research survey, published in the *Journal of Banking Regulation,* tracked market-based and structural indicators from pre- to post-crisis and provides "a narrative for the new landscape in which European banks operate".

When analysing the following market-based indicators, the results showed a decrease in the following figures post-GFC:

- price-to-book ratio;
- realised and implied volatilities;
- credit default swap spreads;
- beta measuring the risk of an entity in comparison with the market; and
- systemic risk indicator, as developed by the Volatility Institute.

This indicates that banks are less safe today than before the crisis.

## LARGEST BANK SETTLEMENTS IN HISTORY

**US$8.5 BILLION**
**BANK OF AMERICA**
*JUN 2011*
Settlement with a group of mortgage bond holders. It is still waiting the approval of a judge.

**US$2.2 BILLION**
**CITIGROUP**
*FEB 2012*
Pays US authorities over claims they used abusive methods to foreclose on homeowners hit by the bursting of the property bubble.

**US$1.5 BILLION**
**UBS**
*DEC 2012*
Fined by US, UK, and Swiss authorities for rigging Libor, and a further GBP30 million for "significant control breakdowns" that allowed a rogue trader to lose US$2.3 billion.

**US$1.9 BILLION**
**HSBC**
*DEC 2012*
Pays US authorities to settle allegations of failure to enforce AML rules exposing the US financial system to drug cartels.

**US$5.29 BILLION**
**JP MORGAN**
*FEB 2012*
Foreclosures settlement.

**US$5.35 BILLION**
**WELLS FARGO**
*FEB 2012*
Foreclosures settlement.

**US$11.8 BILLION**
**BANK OF AMERICA**
*FEB 2012*
Payout relates to the February 2012 foreclosure settlement.

**US$13 BILLION**
**JP MORGAN**
*OCT 2013*
Deal with US regulators to settle claims that it mis-sold bundles of toxic mortgage debt to investors leading to the financial crisis.

**US$16.75 BILLION**
**BANK OF AMERICA**
*OCT 2013*
Settle allegations that it misled investors into buying toxic mortgage securities. The bank said the "claims relate primarily to conduct that occurred at Countrywide and Merrill Lynch" before it acquired them in 2008.

**US$2.09 BILLION**
**WELLS FARGO**
*AUG 2013*
Civil penalties following a federal investigation into its mortgage practices leading up to the financial crisis.

**US$2.6 BILLION**
**CREDIT SUISSE**
*MAY 2014*
Fined for helping some US clients avoid paying tax.

**US$8.9 BILLION**
**BNP PARIBAS**
*JUN 2014*
BNP Paribas admitted to processing thousands of transactions through the US financial systems on behalf of bodies in Iran, Cuba, and Sudan, landing the French bank with a US$8.9 billion fine and leading to the departure of more than a dozen senior employees.

**US$4.9 BILLION**
**RBS**
*MAY 2018*
Penalty by US Department of Justice to end an investigation into sales of financial products in the run-up to the financial crisis, clearing the way for the UK government to sell its 71% stake in the bank.

**SOURCES:** WALL STREET JOURNAL, BUSINESS INSIDER

**+ However, the results were reversed when assessing the following structural indicators in banking, which signalled that banks are safer today:**

- return on assets;
- cost of funds;
- leverage ratio; and
- risk-weight density.

On this seeming contradiction, Basten and Serrano elaborate: "The contrast between the results in market-based and structural indicators can be better framed in comparison with the pre-crisis period. In those years, financial market participants underestimated risks in the banking system and banks themselves were not well prepared to withstand adverse shocks.

"The GFC uncovered these two facts, and in the post-crisis period, we have witnessed a dual significant adjustment: While the regulatory reform has made banks more resilient via increased capital requirements and a binding leverage ratio, financial market participants are now

**In a nutshell, the pre-crisis period could be characterised by high risks in the banking sector which were not priced by market participants, while the post-crisis period seems to be defined by lower risks in the banking sector and market participants fully aware of these risks.**

very sensitive to risks in the banking sector and are adjusting their positions accordingly.

"In a nutshell, the pre-crisis period could be characterised by high risks in the banking sector which were not priced by market participants, while the post-crisis period seems to be defined by lower risks in the banking sector and market participants fully aware of these risks."

Their findings, corroborated by similar research by international bodies like the International Monetary Fund (IMF), define banking today as more resilient than at any other time in modern history. Yet, many outstanding aspects, including the leverage ratio and items on the liquidity agenda, are still works-in-progress.

### INTERCONNECTIVITY AND CONTAGION

Large and interconnected institutions were a key vulnerability.

In the event of a crisis, high interconnectedness – the degree to which banks or markets have connections to other financial institutions, markets, or infrastructure – results in contagion or the 'domino effect' and is a critical systemic risk arising from 'too big to fail'.

In order to identify and properly assess risks of systemic institutions, one of the main developments post-GFC is its classification of globally systemic important banks (G-SIBs) – jointly developed by the IMF, Financial Stability Board (FSB), and Bank for International Settlements (BIS) – that has led to the adoption of a similar classification by other jurisdictions at the domestic level.

Since 2016, classification as a G-SIB – assessed by bank size, interconnectedness, lack of readily available substitutes, global (cross-jurisdictional) activity, and complexity – incurs a systemic capital surcharge of between 1–3.5%. Furthermore, the still-in-progress Data Gaps Initiative, set up by the BIS, is building a common data hub for monitoring systemic institutions, which will give supervisory authorities in major jurisdictions information on risk exposures and interconnectedness across G-SIBs, markets, and jurisdictions.

This development has eased the monitoring of concentration risk in the sector. In particular, the concentration ratio – the degree to which the financial sector is controlled by the largest banks in the system (defined in terms of assets, deposits, or number of branches) – lends insight into the development of the sector's stability, efficiency, and competitiveness.

The IMF's October 2018 *Global Financial Stability Report* (GFSR) found that although systemic institutions have increased their capital buffers and banking systems appear to be slightly less concentrated, competition measures have not improved.

It wrote: "On average, the moderate but sustained decline in the three-bank concentration ratio […] and the size of systemic institutions relative to the economy has been declining or remaining stable in most countries, including those in the Basel Committee on Banking Supervision.

"The trend in concentration has not clearly translated into greater banking competition, as both the Lerner index, a measure of banking sector markups, and the Boone indicator, a measure of elasticity of profits to marginal costs, appear to have markedly increased in recent years."

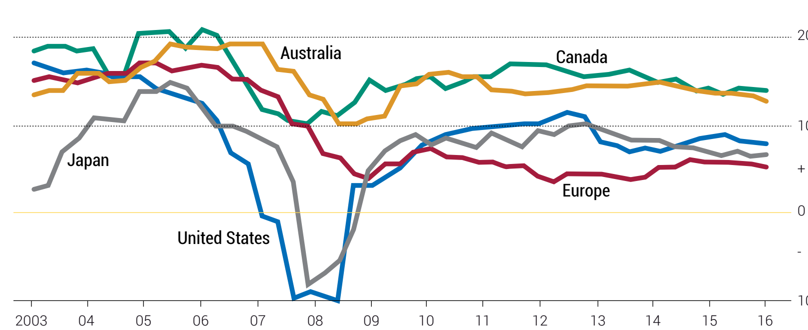
What are we to make of such a situation, i.e. when concentration risk is lower, but competitiveness worsens?

Such a dilemma poses significant pros and cons to the system. Intense bank concentration stalls competition and introduces inefficiencies that, amongst others, reduce access to finance and impair growth. However, it is also proven that concentration arising from mergers and acquisitions can help improve sector efficiencies to drive economies of scale.

How does this then inform policymaking and strategic business decisions?

The impact of concentration and competitiveness measures must be weighed in its totality and not as separate targets. There is no 'one shoe fits all' solution or dedicated mix of policies that will indicate the sector has arrived at an optimal solution.

**CHART 2 BANKS' RETURN ON EQUITY, %**




**SOURCE** MSCI; Thomson Reuters

A continued, refined approach is needed to balance progressive reforms against a build-up of vulnerabilities such as loss of competitiveness and excessive risk-taking. Current numbers indicate that this balance still eludes most in the financial system.

**PROFITABILITY SLIDE**

Under the new regulatory regime, with rising compliance costs and ultra-low interest rates, banks have clocked much weaker financial performances since the GFC.

McKinsey Global Institute's briefing note in September 2018 wrote: "Return on equity (ROE) for banks in advanced economies has fallen by more than half since the crisis. The pressure has been greatest for European banks. Their average ROE over the past five years stood at 4.4%, compared with 7.9% for US banks."


In particular, it highlighted the risk of nonperforming loans' (NPL) drag on the banking system in some emerging markets, citing India's 9% NPL and Turkey's climbing currency depreciation.

It also warns that "banking could become a commoditised, low-margin business unless the industry revitalises revenue growth" from its current annualised revenue growth of 2.4%, trailing far behind to its 12.3% pre-crisis level.

To arrest the decline, some incumbents have successfully adopted fintech innovations – namely, machine learning, blockchain, application programming interface – as part of their new operating model, whilst others relied on more traditional austerity measures such as bonus cuts and reskilling its workforce.

Significantly, the best performing banks in the post-crisis era have dramatically pared operational costs even whilst strengthening risk and compliance headcount.

**NEW THREATS**

As the spectre of the GFC recedes as a distant memory, reform fatigue has inevitably set in. Certain quarters have called for a rollback of macroprudential oversight, an unwise move given the emergence of new threats and priorities in this ever-changing landscape.

In the spaces of fintech and cybersecurity, vigilance is necessary. Digitalisation has raised red flags on all fronts as cyberthreats become increasingly stealth-like and sophisticated in their manoeuvring, posing threats to financial stability.

The most complex challenge in this sphere is aptly described by the FSB as supporting "fintech's potential contribution to innovation, efficiency, and inclusion, while safeguarding against risks that could amplify shocks to the financial system".

But the most crucial warning comes from the IMF with regard to the rising systemic risks of new forms of shadow banking and market-based finance: "In many countries, systemic risks associated with new forms of shadow banking and market-based finance outside the prudential regulatory perimeter, such as asset managers, may be accumulating and could lead to renewed spillover effects on banks. This is particularly true in many emerging markets, including China, where shadow banking has grown rapidly, albeit from a small base."

"Numerous policy and regulatory options for reducing shadow banking risks could be envisaged, including activity-based (as opposed to entity-based) regulation and development of macroprudential tools for nonbanks."

**ZERO-FAILURE DOESN'T EXIST**

Economist Nouriel Roubini – once labelled a 'Cassandra' after the Greek character's namesake who held both the gift of truthful prophecy and curse of never being believed – was one of the few who predicted the housing bubble crash of 2007 and panned by critics.

Today, the tables are turned and his forecast that "by 2020, the conditions will be ripe for a financial crisis, followed by a global recession" has made headlines and raised alarm bells in financial markets.

But are we really that surprised? For those who remember and have weathered the storms of multiple crises, the near-rhythmic 10-year boom-bust cycle is inevitable. However much we fear it, the cycle of expansion and contraction is the natural order of markets.

Zero-failure is an unrealistic expectation. Neither is it the objective of the numerous safeguards put in place since the GFC.

The course for banking's True North – greater market resilience, higher standards, enhanced codes of moral conduct – was not set to avert a future crisis, but to withstand it.

Will our efforts to enhance market resilience make any difference in the next financial crisis? Time will tell as to how banking weathers its next 'perfect storm'. ✱

■ *Angela Yap is a multi-award-winning entrepreneur, speaker, author, writer whose work has been featured and referenced in international journals and magazines. She is the founder of content research firm, Akasaa.*

# CENTS AND SUSTAINABILITY

SUSTAINABILITY IS INCREASINGLY RELEVANT TO THE FINANCIAL SERVICES SECTOR, DRIVEN BY ETHICS AND PROFIT. HOW HAVE FINANCIAL INSTITUTIONS PERFORMED AND JUST HOW FAR ARE WE BANKING ON SUSTAINABILITY?

**Promoting** higher levels of financial inclusion is also a positive sum agenda: In addition to potentially reducing poverty, the banking industry can capitalise on the shared prosperity to be gained from serving the global bottom 40% whose spending power is set to nearly double from US$3 trillion to US$5.8 trillion.

With populations booming and resources dwindling, resilience and sustainability have increasingly become the name of the game. Sustainability as a trend has been on the upswing at least since 2008's global financial crisis (GFC), when the great game of global finance saw a reorientation towards generating shared prosperity and economic growth without compromising future resources.

International financial institutions (FIs) like the World Bank (WB), International Monetary Fund (IMF), and Asian Development Bank (ADB) set the course by supporting the United Nations' (UN) Sustainable Development Goals (SDGs). Building on the Millennium Development Goals, the SDGs have 17 goals that range from minimising inequalities (no poverty, gender equality), ensuring better quality of life (clean water and sanitation, affordable and clean energy), and more sustainable living (climate action, sustainable cities and communities), to equitable prosperity and economic growth (industry, innovation, and infrastructure).

Despite the big push, performance has been mixed so far. Global finance has a plethora of actors, but not all — private FIs and investors in the ASEAN region included — have had a significant presence on the sustainability stage.

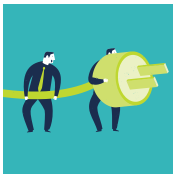
This is perhaps surprising, given both the cents and sense sustainability makes. On one hand, the Business & Sustainable Development Commission estimates that achieving the SDGs in just four key areas — food and land use, cities, energy and materials, and health and well-being projects — will add US$12 trillion to the global economy in business savings and revenue by 2030.

By riding the SDG wave, FIs will be well-poised to tap into megatrends such as the growing demand for quality healthcare for ageing populations — a potential gold mine for insurance. Promoting higher levels of financial inclusion is also a positive sum agenda: In addition to potentially reducing poverty, the banking industry can capitalise on the shared prosperity to be gained from serving the global bottom 40% whose spending power is set to nearly double from US$3 trillion to US$5.8 trillion.

Inertia, on the other hand, has immense costs. Ignoring climate change alone could devalue financial assets by US$2.5 trillion, according to scholars at the London School of Economics.

## GETTING IN ON THE ACTION

Already cottoning on, some FIs have adopted the sustainability drive early. Efforts in the poverty reduction sphere have especially gained momentum, given that this SDG links well to financial inclusion and financing poor communities for upward mobility. One example would be South Korea's Shinhan Financial Group, which offers guarantee-and-collateral-free small loans to communities with low



**Despite the big push, performance has been mixed so far. Global finance has a plethora of actors, but not all – private FIs and investors in the ASEAN region included – have had a significant presence on the sustainability stage.**

income and low credit scores.

Another player wading into the sustainability pool is Grab. In April 2018, the ride-hailing company launched microfinance options via its fintech platform, Grab Financial. Given Grab's extensive reach in Southeast Asian markets, growing data pool, and Big Data capabilities, it may afford large segments of ASEAN's unbanked and underbanked with financial access.

What this means for FIs is less clear; some competition may drive higher sustainability levels, but whether Grab will be a victim of its own overstretch remains to be seen.

Platforms for sustainable finance and impact investment are also flourishing within the region. Supported by the Monetary Authority of Singapore, the World Wildlife Fund (WWF) has created the Asia Sustainable Finance Initiative to channel financing towards projects with positive economic, social, and environmental effects. Credit Suisse, Dutch FMO Bank, ING Bank, and the UN Development Programme-UN Social Impact Fund (UNDP-UNSIF) have also spurred a similar project, the Sustainable Finance Collective Asia. Closer to home, WWF has also partnered with eight Indonesian banks for the Indonesia Sustainable Finance Initiative, a national impact investment platform.

On the government-to-business partnership front, the ASEAN Financial Innovation Network (AFIN) was also launched in late 2017. A fintech sandbox, AFIN aims to match fintech companies with financial institutions to plug regional financial inclusion gaps in less developed markets.

**What this means for FIs is less clear; some competition may drive higher sustainability levels, but whether Grab will be a victim of its own overstretch remains to be seen.**


**PEDAL TO THE METAL**

Still, critical mass is not yet on the horizon. Existing initiatives and projects need to be revved up and better targeted if a sustainable 2030 is to materialise.

At almost US$300 trillion in total stock of global financial assets, UNDP Administrator Achim Steiner, in a speech on 18 November 2017 to development financing delegates, acknowledged that a shortfall of capital is not the issue. "However, currently the global financial system is not channeling those vast sums effectively towards investments for sustainable development and achieving the SDGs."

In SustainAbility's *Global Trends & Opportunities: 2016 and Beyond* report, Stefanos Fotiou, Chief of Environment and Development Division at the UN Economic and Social Commission for Asia and the Pacific, emphasised, "If there is one sector we should ask more from, it's the finance sector."

FIs have to rise above and beyond standard practice to pursue sustainability more holistically and comprehensively. ASEAN banks, for instance, tend to interpret corporate governance codes pertaining to environmental and social policies as encompassing only their own footprint.

Targets such as energy efficient buildings are a step forward. But infusing sustainability-mindedness into investment and financing decisions should be top of the list.

"If banks started using serious sustainability criteria in terms of how they evaluate loans and combine their portfolios," Fotiou added, "many changes would follow."

FIs can, in this sense, design their core bread-and-butter activities to consider and target SDGs. One way forward would be to utilise the Inter-Agency and Expert Group on SDG Indicators. Operationalised since 2016, the indicators break down abstract SDGs into 169 quantifiable and integrated targets. Annual progress reports mean that data for existing efforts are consistently accounted for.

In this sense, FIs and other stakeholders can better target unserviced and underserviced goals. Under Goal 1 of eradicating poverty, for example, FIs can take on more projects that go beyond financial inclusion. Instead, more financing could be channelled into areas of disaster insurance for vulnerable populations, sharing data to create more robust land rights systems, or strengthening tax collection for SDGs by heightening cooperation with states on matters of tax evasion and money laundering.

Some FIs have already begun

moving in this direction. In late 2017, Wilmar International took on the first sustainability performance-linked loan in both Asia and the palm oil industry from ING Bank by converting a portion of its existing US$150 million revolving credit (RC) facility. If sustainability KPIs are met, as tracked by research firms like Sustainalytics, Wilmar will receive reduced interest rates for its loan in the following year.

Wilmar followed this up by accepting another US$100 million RC sustainability performance-linked loan with DBS Bank in August 2018.

In March this year, Olam International, another commodities firm, also received a US$500 million club loan facility contingent upon it meeting various environmental, social, and governance (ESG) metrics.

Another option to advance sustainability is for FIs to continue pursuing public-private partnerships (PPPs) and blended finance initiatives currently in play. Even then, certain targets such as financial inclusion are intimately tied to banking and finance. Hence, while it can be easier for FIs to aim for certain goals, this potentially sidelines other SDGs.

Overall, however, while PPPs can enhance data cooperation and identify more bankable projects, SDGs are public goods that cannot always be bankable. Moving away from shareholder-heavy to a more comprehensive stakeholder-focused model, along with prioritising holistic long-term value rather than short-term profit, will be key to mobilising higher SDG participation from FIs.

But without streamlined regulation, incentives for sustainable investing are limited.

There is some light at the end of the tunnel. With economic policymaking increasingly incorporating SDGs, sustainable finance is likely to accelerate. This is already on track in regions such as South Asia (see box story on page XX).

In March 2018, the European Commission adopted the Action Plan on Sustainable Finance. As banks align their investments to meet new regulatory

## THE SUSTAINABILITY RAJ

South Asia is having its renaissance in sustainable policymaking.

India is the first emerging economy to track SDG progress and general quality of life at the state level under its Social Progress Index.

In addition to national-level policies, the region has also held the annual South Asian Speaker Summit on Achieving the Sustainable Development Goals since 2015. The last leg of the summit held in Sri Lanka prioritised green growth strategies, access to education, and inclusive societies.

The multilevel governance approach has also influenced sustainable business practices at FIs like YES Bank.

In June 2018, India's YES Bank launched the country's first Green Deposit, with proceeds raised through these bonds being channelled to SDG-aligned sectors. Its enhanced sustainability reporting also began in June.

> The multilevel governance approach has also influenced sustainable business practices at FIs like YES Bank.

This makes YES Bank one of at least 150 FIs globally to support the Financial Stability Board's industry-led Task Force on Climate-related Financial Disclosures.

In May, the bank partnered with local state governments in Rajasthan and Haryana to improve financial and digital literacy among 10,000 farmers, in addition to spreading good agricultural practices for more efficient farming in line with the 'Doubling Farmers' Income by 2020' national drive.

Late last year, YES Bank also launched its 'Say Yes to Sustainable MSMEs in India' campaign to spread energy-efficient practices among Indian MSMEs, which contribute to 70% of India's industrial pollution.

Consequently, YES Bank has made its way into *Forbes* 'Global 2000' list and has been ranked in the top 12% of banks according to ESG indicators by OEKOM Research AG.

A lack of demonstrated success also hinders local banks from growing their impact investment portfolios, according to the Global Impact Investing Network's *The Landscape of Impact Investing in Southeast Asia* report. However, with more and more FIs jumping onto the sustainability bandwagon, financial services practitioners in the region should dip their toes into the sustainability pool.

standards, this will have ripple effects elsewhere around the world.

ASEAN itself has yet to harmonise national ESG codes and sustainable finance regulations. It has, however, recently released the ASEAN Green Bond Standards in an attempt to further regulate and channel finance towards SDGs. In January this year, Bank Negara Malaysia created the Guidelines on Sustainable and Responsible Investment, a national regulatory framework for sustainable investment.

A lack of demonstrated success also hinders local banks from growing their impact investment portfolios, according to the Global Impact Investing Network's *The Landscape of Impact Investing in Southeast Asia* report. However, with more and more FIs jumping onto the sustainability bandwagon, financial services practitioners in the region should dip their toes into the sustainability pool.

Looking beyond Asian shores is another option. The world's largest sovereign wealth fund, Norges Bank Investment Management, actively avoids investing in sustainably questionable activities, adding relevant partners and projects to their list of sin stocks. It also initiated dialogues with Malaysian and Indonesian banks over their palm oil financing activities.

BNP Paribas recently entered a partnership with the World Bank and Switzerland's SYZ Bank to offer an equity bond that links investment returns to the performance of SDG-driven companies. Around 15% of its loans worldwide have been channelled to SDG-promoting projects; out of 13 company-wide corporate social responsibility (CSR) indicators, nine are used to determine the variable incentive plan for the Group's 5,000 top managers.

Elsewhere, Dutch Rabobank has also committed US$1 billion to "provide grants, de-risking instruments and credit to clients involved in sustainable agricultural production, processing or the trade of soft commodities provided they follow strict provisions for forest protection, restoration and the involvement of smallholders."

For impact investing to take full flight, traditional preferences for philanthropic giving have to make way for sustainable finance. Even in global financial centres like Hong Kong, a lack of awareness and preferences for traditional CSR or philanthropy are some barriers to greater buy-in for sustainable finance.

Efforts to achieve the SDGs will also be undermined if FIs engage in 'SDG washing'. Banks should avoid simultaneously engaging in unsustainable projects and championing only certain SDGs. For instance, despite adopting sustainable financing guidelines, the DBS-OCBC-UOB trifecta are significant regional financiers of coal projects. Even the Asian Infrastructure Investment Bank, which positions itself as a 'green' bank, recently financed its first coal plant in Myanmar; over the years, the World Bank's private sector arm, the International Finance Corporation, has also come under fire for similar charges of fuelling coal power booms in Asia.

Both private and public sectors can do more in this regard. Lip service alone will not bring the SDGs to life. Adopting sustainability principles in name must be complemented with adopting it in practice: For example, FIs can begin reporting impact measurement, as promoted by the Global Impact Investing Network.

Having disclosures according to quantifiable metrics will go a long way towards making SDGs more investable. As Wilm Van Hyfte, Global Head of Responsible Investments at Candriam, noted at 2018's Sustainable Investment Forum: "When these things become measurable, they become manageable. And then investors can then price it."

**HEAVY LIFTING**

At this point, the sustainability finance field has fewer early adopters and less profitability than desirable. Yet it is the road less travelled that makes all the difference, and that difference must be made soon.

FIs are but one component of a wider world and existence. They are, however, collectively in a prime position to make a deeper difference. Better finance can save the world, but FIs need to be willing to not only wear the cape but also do more heavy lifting for that to happen. ✱

■ *Amalina Anuar is a Singapore-based writer interested in political economy, international relations, and comparative integration between Europe and Asia.*


ASIAN
INSTITUTE OF
CHARTERED
BANKERS

# Big Data meets Big Brother

**Technology to reduce harmful gambling promises to deliver social good. But how far should banks go to control customer spending? Are we edging closer to China's 'social credit' system, which scores consumers on good or bad behaviour?**

With so much valuable customer data available to banks, the question of ethics is never far away. Every financial transaction leaves a digital footprint that can be accessed – and shared. So how should banks be using this data?

It's a question that the gambling and betting industry has been examining in depth. Once characterised by smoke-filled bookies frequented by men, the industry and its

demographics have been transformed by online gambling.

Today, more than half of the UK's gamblers – 51% – place bets using mobile phones and tablets, according to research from the Gambling Commission, which regulates the industry to safeguard consumers. The commission also finds that 41% of women and 48% of men have gambled in the past four weeks, while 97% of online gamblers gamble at home.

So technology has widened access to gambling and made it available 24/7. But technology can also help – particularly where online gambling has become a serious addiction. This is an issue that challenger banks Starling and Monzo have taken steps to address.

## SELFLESS TECH?

Starling has introduced a voluntary gambling blocker feature on its app which allows customers to stop their card being accepted for betting transactions. For someone who's looking to curb their addiction, this is a much easier process than contacting all the places they may be tempted to place bets and asking each one individually to refuse their card.

Monzo is developing a similar feature and meantime signposts customers who tell it about a gambling problem to sources of support, including GamCare, a charity providing free software that blocks online gambling sites.

Both banks cite research from the Money and Mental Health Policy Institute, an independent charity committed to breaking the link between financial difficulty and mental health problems. It found that placing an obstacle between people and the sites they find problematic can be a useful first step in helping users regain control over their financial lives.

"This research, combined with conversations with customers, has led us to launch this feature which gives all customers the choice to block spending by card on gambling and betting," said Starling when it introduced its merchant blocking feature. "This includes betting shops and horse racing tracks, as well as gambling websites such as online casinos and betting exchanges."

Starling believes other banks will follow suit, but feels wider support for problem addiction must be left to specialists. "We are a bank, not trained addiction counsellors," says Alexandra Frean, Starling's Head of Corporate Affairs. "However, we want to offer customers a tool that helps them make a positive choice about how and where they spend their money."

## OPEN ETHICS

On the wider ethical considerations of monitoring how customers spend their money and sharing account details with other providers, Starling feels the industry has a duty to ensure that customers give informed consent. "This is a difficult task because it's not enough to get them to click on an 'I Agree' button," says Frean.

"Consumers might not understand how valuable or sensitive different parts of their data could be. The industry has to educate and empower customers to make sure that consent is meaningful."

Open Banking can be a force for good and a real game changer for the way individuals and businesses manage their finances, Frean believes. But many people still don't seem to understand what it is: "There's a huge need for education around the subject, but we think that the public is open to learning about it and embracing it," she states.

**+ Monzo is developing a similar feature and meantime signposts customers who tell it about a gambling problem to sources of support, including GamCare, a charity providing free software that blocks online gambling sites.**

Both banks cite research from the Money and Mental Health Policy Institute, an independent charity committed to breaking the link between financial difficulty and mental health problems. It found that placing an obstacle between people and the sites they find problematic can be a useful first step in helping users regain control over their financial lives.

This has included looking at how giving consumers greater control of the way they use financial products could work alongside the existing protections that we require gambling companies to provide, such as offering consumers the option of blocking their cards from gambling companies.

**Tim Miller**
*Executive Director of the Gambling Commission*

The Gambling Commission's 2017–2018 annual report estimates that 430,000 adults are problem gamblers, while 2 million adults are 'at risk' of experiencing problem gambling.

## GREATER CONTROL

Tim Miller, Executive Director of the Gambling Commission, believes the steps taken by Starling and Monzo will have a positive impact. "We've been actively talking to financial institutions about the role they could play in protecting customers who are struggling with their gambling," he says. "This has included looking at how giving consumers greater control of the way they use financial products could work alongside the existing protections that we require gambling companies to provide, such as offering consumers the option of blocking their cards from gambling companies."

In each gambling sector, the Commission says it has driven the establishment of 'multioperator self-exclusion schemes', which allow customers to issue a single request asking operators to take all reasonable steps to prevent them from gambling. "A complementary initiative to allow customers to block their bank or credit cards should help support a reduction in harm," he adds.

As part of its review of online gambling published in March, the Gambling Commission is also taking a closer look at gambling with credit. "We will consider prohibiting or restricting the use of credit cards for gambling and the offering of credit by gambling businesses, but will explore the consequences of doing so," Miller says.

## STAR TREK STATE

The answer to that, according to Julian Gruin, a political economist and Assistant Professor of Transnational Governance at the University of Amsterdam, is yes. "As individuals and businesses increasingly conduct their financial business through integrated online systems, banks have both greater opportunity and more incentive to monitor, manage and manipulate financial activity and the movement of capital," he argues.

"Big data technologies enable banks to start constructing complex and increasingly comprehensive images of financial flows, which will lead to a version of what Andy Haldane, Chief Economist at the Bank of England, described as his dream of a 'Star Trek chair and a bank of monitors…tracking the global flow of funds in close to real time'."

But instead of identifying patterns that might lead to systemic risk, this form

## TIP OF THE ICEBERG?

While technology that helps prevent problem gambling is welcome, there are ethical questions about how far the monitoring of customer behaviour should go. In China, for example, the development of a so-called 'social credit' system has prompted incredulity – and growing concern – internationally. Due to be fully operational by 2020, it uses big data, artificial intelligence and mass surveillance to monitor China's huge population.

The system, first announced in 2014, scores citizens based on their behaviour and penalises them for infractions such as smoking in no-smoking areas, bad driving, not paying bills on time or spreading fake news. According to reports, punishments can include restricting plane or train travel; slowing the individual's internet speed; and blocking their access to education, jobs and hotels. By monitoring Chinese citizens abroad – as well as international companies doing business in China – the social credit system could also start to spread beyond the country's borders, some observers believe.

So is monitoring how customers spend their money just the thin end of the wedge for the banking industry?

of 'algorithmic governance' would be able to identify patterns that influence a bank's operations at numerous levels, from marketing to risk assessment, Gruin believes.

Although China's social credit system is at a very early stage of development, this kind of 'Big Brother' surveillance using big data is on its way, he adds. "The Chinese case is unique in its combination of several factors, including the vast public resources being poured into machine learning and artificial intelligence technologies," Gruin says. "China also has a resilient and sophisticated authoritarian government that has immense control over the country's private tech industry. And Chinese society is positively disposed to governance models that use technology to increase public trust in areas such as environmental, consumer and financial regulation."

In other countries, Gruin suggests, we might expect to see systems of social and economic 'dataveillance' that contain "a different admixture of private and public control, and which will have more or less explicit political implications".


### CARROT OR STICK?

Chris Cowton, Professor of Financial Ethics at Huddersfield Business School, argues instead for a distinction between banks monitoring how customers spend their money on the one hand and helping customers to control their spending on the other. "I think it's perfectly reasonable, indeed commendable, to allow a problem gambler to block payments," he says. "Gambling addiction wrecks lives, both the gambler's and that of others. The blocker technology is just another tool in that person's armoury to help in moments of weakness, such as banning themselves from betting with certain companies or blocking access to certain websites."

**Gambling addiction wrecks lives, both the gambler's and that of others. The blocker technology is just another tool in that person's armoury to help in moments of weakness, such as banning themselves from betting with certain companies or blocking access to certain websites.**

Cowton doubts that a social credit-style system like China's will be arriving in the West any time soon. "Such a system would be built on the particularities of China's culture and I would be surprised to see something similar take root in countries such as the UK," he suggests. "I think incentive schemes are much more likely to be privately led or, at least, focused on particular issues. Healthy eating might be a good example. However, I'd be surprised if this were to involve the banks, with reward provided through preferential interest rates – which would probably appeal more to the 'healthy wealthy', anyway."

While banks aren't obliged to help customers with addiction problems, technology puts them in a position to assist, particularly in relation to gambling. "There doesn't seem much they can do to help someone with a drug habit, for instance, and in the case of an alcoholic, it's impractical to block shopping at the supermarket or buying alcohol with cash," Cowton points out. "But in the case of gambling, very large debts can be built up quickly, which is why the bank is in a good position to help."

He suggests the ability for third parties such as mortgage lenders to see how a customer is spending their money should be restricted to a small number of problem cases. "I think confidentiality is a good principle for anyone involved in the management of someone else's financial affairs. If there are particular reasons for opening up a customer's account details to lenders, it has to be with the customer's permission, for the customer's benefit, and something seen in only a small minority of cases. This latter point will help to ensure it really is for the customer's benefit." ✱

■ *This article was previously published in the Chartered Banker Magazine, October/November 2018.*

BY RADISH SINGH

A BALANCING ACT IN

# Trade-Based Money Laundering Compliance

The complexity in trade-based money laundering compliance…to trade or not to trade?

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

Consequentially, financial institutions (FIs) have been facing much difficulty in monitoring and implementing controls in their trade finance business to combat trade-based money laundering (TBML). The problem has been further exacerbated by a lack of clarity in the compliance requirements and regulatory expectations in many jurisdictions.

Whilst controls can be put in place for documentary trade, greater issue lies in open account situations where the FI has far less visibility on the underlying transaction. In documentary trades, regardless of the letter of credit (LC) meeting international and legal standards, where there are TBML and economic sanctions issues, it may still warrant an action from the FIs to report or otherwise take necessary steps to protect the FI, and requires the balancing art of "not tipping-off".

Surely, the unintended consequences of the heightened risk-based approach and regulatory expectations is not to stifle global trade that, in turn, can hurt global commerce by, inter alia, reducing export volumes and increasing transactions cost. There certainly is a legitimate call to balance regulatory wish lists and commercial needs for global trade to thrive. As it stands, the margins for trade

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

transactions for FIs is thinning rapidly, attributable to competition and escalating compliance cost.

Some key challenges highlighted here include those provided in the Banking Commission of the International Chamber of Commerce (ICC), Bankers Association for Finance and Trade (BAFT) and Wolfsberg Paper on TBML and our experience of working with the industry. Deloitte believes that these resonate with FIs given the operational difficulties they encounter. This also follows the release of the industry paper, *Best Practices for Countering Trade-based Money Laundering,* on 14 May 2018 by Singapore's Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership.

## WHAT IS THE GLOBAL REGULATORY STANDARD?

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

These, at best, are recommendations of best practice and require force of local legislation or regulations. Key regulators that have set the tone on regulatory expectations are the Monetary Authority of Singapore (MAS) and Financial Conduct Authority, United Kingdom. Few others have set the tone through inspections conducted.

Though myriad references are found on the best practices and regulatory expectations, the issues still remain in operationalising and implementing these requirements or best practices. In addition, the global footprint of FIs and cross-border trades bring with it the challenge of harmonising compliance standards for FIs given that only a handful of regulators have issued guidance for the industry. The question remains on which is "the standard" that FIs should imbibe, that is recognised and enforceable by their home or host regulator.

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

## KEY CHALLENGES

### + Getting the Price Right

The regulatory expectations generally are that FIs should assess the reasonableness of the price of goods quoted when facilitating trade transactions. The issue faced by the industry is the lack of reliable and publicly available statistics and data on prices of myriad of goods, except, arguably, commodities. Complexity in price assessment is added when goods traded are, for example, spare parts and constituents or otherwise components of larger (and potentially specialised) items. An international agreement on the level of diligence needed by FIs for "price checks" will help. This should really be based on a defined risk-based approach of an FI. For example, where the customer is a known reputable business or has a long standing relationship with the FI or the price variation is within acceptable range (based on standards developed using the FIs own data on transactions), intrusive price check may not be an automatic action to take, unless there are anomalies noted or the price variation is not within an acceptable range. FIs may also establish their own internal database for price guidance based on the transactions handled by the FI. Greater level of transparency can be achieved if governments, regulators or enforcement agencies and trade bodies partner with FIs to share information and establish a single, consolidated pool of commodity prices, as was recommended by ICC, BAFT, and Wolfsberg.

**+ Know the Goods Transacted**

Specialist knowledge is often required to determine whether goods involved in transactions have dual-use. FIs typically have limited knowledge to ascertain this. Dual-use goods include software, technology, documents and diagrams, which can be used for both civil and military applications. The goods can range from raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. They could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers. It is common that trade documents do not provide a detailed description of the goods or components of the same. A good practice is to generally screen goods (using preferably a paid database) to ascertain whether they have dual-use and using this with the FIs profile of the customer and knowledge of the customer (where information should have been gathered at the onset on the goods intended to be traded), details of the transactions conducted by the customer and parties involved, length of the relationship and the issues seen during the life cycle of the customer. The FIs may need to take a heightened risk approach with a new customer relationship where the goods traded are capable of dual-use.

**+ Import/Export Licensing**

FIs are generally not always in a position to determine if an export licence is required for a trade transaction. The counterparties to a trade transaction are in a better position to determine that an export licence is required and obtain such licence if it is required. At best, FIs can obtain advice on the typical goods that require such licences in key jurisdictions that they have exposure to via their customers and transactions,

and seek their customers' confirmation that, where required, such licence has indeed been obtained.

**+ Detecting Duplicate LCs, Bills of Lading (BL) and Invoices**

The question is how will FIs even know, under normal circumstances, that a customer is submitting duplicate or fraudulent trade documents? FIs only have access to their own information and not that of other FIs. Hence, their holistic or global view on a transaction and its documentation is limited. The best practice is to check with the issuing bank when an FI is presented with trade documents, sight the original documents and check for any obvious anomalies in the documentation, over and above screening the parties involved. Relying on an MT700 message alone may not suffice. If multiple banks are seeking confirmation from the issuing bank, it should trigger a red-flag review on the part of the issuing bank who can alert the other banks and take necessary action.

## CIRCUMVENTED YET AGAIN?

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

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

## STILL STUCK IN PAPER-BASED TRADE FINANCE?

Despite the level of technology available, trade finance processes continue to be largely paper-based. This reduces the FIs' efficiency and effectiveness in implementing risk management controls.

Continued need for manual input and review or monitoring of trade transactions is a tedious task prone to human error and, arguably, inadvertent human misjudgment. FIs with large trade books suffer from costly and time intensive manual review of paper documents.

Today, there clearly is a lack of holistic view of the information flows in trade transactions and seamless capability to spot red flags in a systematic manner. Ideally, the developments we do need to urgently witness across the industry are (in no particular order):

- digitisation of trade documents to reduce human error and expedite the process while decreasing the costs of manual trade documents and transactions review;
- technological developments to fully automate trade transactions and implement pattern-based recognition systems (which, if at all, may only be attainable to larger FIs) or a fully automated trade solution that tracks the transaction which performs screening, checks on vessel routes, and assess red flags from data on the customer, documentation, transaction, shipment and payment, until the transaction is completed – with human intervention, analysis and judgment as required; and
- a blockchain solution across the industry to create a sustainable ecosystem for all parties to a trade transaction – as a utility that tracks a transaction based on digitised uniquely identifiable trade documents (we are hopeful that this materialises) and BLs (ideally).

## WHAT'S NEXT?

With the growth in the volumes of international trade and given the complexity of the trade finance business, improving TBML compliance measures and controls require a collaborative effort between relevant agencies and FIs.

To summarise, global and inter-agency cooperation is needed with the industry on:

- Creating global trade data for price-checking purposes.
- Agreeing on the reasonable standards for due diligence required on the part of the FI with regard to dual-use goods. Practically, unless it is an outright red flag or a weapon of mass destruction, it is quite difficult to determine whether some items are going to be used for dual or wrongful purpose. For example, certain chemicals or chemical content of goods such as fertiliser, cannot always be concluded as being intended for dual use by a customer whose business is to manufacture chemicals or fertilisers or otherwise by a customer who has an established need or use of these in their customary business.
- Policy shift towards including key parties in a trade transaction to also play their part – the rules should equally apply to importers and exporters (for example, pre-registration with customs before these parties can conduct international trade, which pre-registration should be reliable for the use of FIs); importers and exporters should conduct Know Your Client/ Customer Due Diligence (KYC/CDD) on their clients; shipping companies should check on the buyers and sellers, goods being transported and ensuring that International Maritime Organization numbers are provided on the BL and insurers to conduct CDD on the parties at the same standards that FIs do for trade transaction purposes.
- Customs authorities possibly mandating unique identifiers for goods imported and exported, dual-use goods and restricted or embargoed goods should require pre-certification from customs before the use of any banking facilities and monitoring of tugboats feeder vessels use. For example, mandating the provision of the Harmonised System Classification of Goods and International Maritime Dangerous Goods Code to assist banks in screening goods or assessing red flags related to goods.
- A global agreement on TBML regulatory standards, which are harmonised across all jurisdictions to create clarity for FIs and a level playing field regardless of location of the FI and size of business given that the risk remains the same.
- Establishing a Trade Transparency Unit, which will enable the global partnership to leverage trade data as well as import/ export data from other participating countries to effectively analyse trade information.
- Doing more to streamline procedures to help detection of duplicate BL where shipping companies could potentially "centrally" register a BL they have issued which can be checked by the bank for authenticity.
- Given the complexity of trade transactions (and transactions monitoring globally), regulators and enforcement agencies could support an initiative to conceptualise an industry-wide surveillance system where an FI should be able to holistically view or visualise a trade transaction and parties involved in the same. This should, in turn, sharpen the ability of the FI to conduct transactions monitoring or surveillance and red-flag detection based on the information and data available. The current impediment faced by the industry is that a given FI has only a limited view of a small part of the transaction, which is not always helpful in detecting anomalies and red flags. ✱

**WE URGE FOR INTELLIGENCE SHARING** across regulatory and enforcement agencies, and the industry as an imperative way forward. Needless to say that resources spent on KYC/CDD, transactions monitoring and manual reviews conducted by FIs is not producing the intended results in all cases despite much effort. Accordingly, a paradigm shift in the manner in which surveillance is undertaken has to change to become cutting-edge with greater public-private partnership and, ultimately, creation of an ecosystem for a global view of trade transactions, as suggested above.

■ *Radish Singh is Partner, Deloitte South East Asia Financial Crime Leader Singapore.*

BY KANNAN AGARWAL

# How Well Can You Keep A Secret?

With the rise of new data privacy laws, banks must precariously **balance confidentiality obligations** against Open Banking commitments.

Data sovereignty – the idea that data are subject to the laws and governance structures within the nation it is collected – is being redelineated as we speak. Many privacy laws, drafted decades before the advent of the internet and digital media, have undergone revisions, updates, or complete overhauls.

Banking today is no longer just about shutting access and keeping information a secret.

The bank of the future must guard sensitive information without sacrificing its pledge to adhere to competition laws, open information architecture, and transparency.

**+ The bank of the future must guard sensitive information without sacrificing its pledge to adhere to competition laws, open information architecture, and transparency.**

### TWIN-CHARGED

Globally, the onward charge in data privacy laws is led by two crucial EU-enacted regulations that enforce minimum standards of care in customer data protection and rights:

+ **General Data Protection Regulation (GDPR).** Considered to be the framework for global data privacy, GDPR came into effect on 25 May 2018 and replaces the former Data Protection Directive. The regulation applies to all processing of personal data of EU citizens, even when processed by a non-EU entity, with non-compliance resulting in fines up to EUR20 million or 4% of the organisation's annual global turnover.

+ **Payments Services Directive 2 (PSD2).** Dubbed the 'Open Banking' regulation and drafted with the intention of opening up financial services to increase sector competition and innovation, this legislation came into effect on 13 January 2018. It mandates that banks give qualified third-parties – fintech, large technology firms, other banks, and retail organisations – automated access to customer transaction accounts to lower customer costs and enhance merchant flexibility. Banks must make their application programming interfaces or APIs – software

In terms of progress with respect to which processes were brought into compliance first, the respondents are furthest along with customer-facing processes such as cookie consent management and individual rights management, and most behind on non-customer facing issues such as international data transfer mechanisms and vendor management.

that allows independent systems to communicate with each other – open in order to allow these third-parties to develop new products and services, and keep integration costs low. Failure to do so would be considered a breach of competition laws.

When applied in tandem, these two standards represent the conundrum in Open Banking. At face value, both laws uncategorically state that individuals own their personal data and should be given the right to choose how it is shared and with whom. However, obtaining consent to the right to data portability – the sharing or transfer of personal data from one IT environment to another in a safe and secure way – is grey area.

GDPR guidance states that data controllers, i.e. banks, are responsible "to ensure that they genuinely act on the data subject's behalf" but PSD2 imposes more stringent protection and allows only for access to information "explicitly requested by the customer". As a result, many predict that a two-part process for consent – first obtained by the third-party with subsequent confirmation by the bank – will prevail as the predominant standard of care.

Also, the high punitive damage threshold under GDPR may lead to overly strict interpretations of consent that run counter to PSD2's spirit, dampening the objective of Open Banking to increase competition and lower costs for financial services.

The solution, thus far, in the months since 'go live' of both laws, is for banks to avoid silo implementation and ensure coordination between teams tasked with data privacy enforcement.

**STATE OF COMPLIANCE**

Data privacy management firm TrustArc's July 2018 research report, *GDPR Compliance Status: A Comparison of US, UK and EU Companies,* turned up with some surprising results just two months after the regulation's go live.

Despite the hefty price tag for GDPR compliance, a majority of survey respondents felt the journey was worthwhile. TrustArc reported that 65% of respondents view GDPR as having a positive impact on their business with 15% to the contrary, 68% clocked spending in excess of six figures, and 67% expect to spend an additional six figures by end-2018.

"Contrary to the common view that the fear of GDPR fines would be the prime motivator for companies to become compliant," wrote the management firm, "the respondents overwhelmingly cited support of their corporate values, and meeting the expectations of their customers and partners as the primary drivers."

"In terms of progress with respect to which processes were brought into compliance first, the respondents are furthest along with customer-facing processes such as cookie consent management and individual rights management, and most behind on non-customer facing issues such as international data transfer mechanisms and vendor management."

**INTERCONNECTEDNESS**

Although GDPR and PSD2 don't ring a bell for many in Asia, its influence in national data privacy regulations in this part of the world is certainly tangible as many countries have already ramped up existing laws to achieve equivalent standards, with the most notable being:

Japan's Act on the Protection of Personal Information, which dates back to 2003 with extensive reforms passed in 2015 by the National Diet. The EU has added Japan to its whitelist of compliance-approved countries, giving the green light to transfers of personal data between the EU and Japan without the need for instruments such as standard contractual clauses, binding corporate rules, or privacy certifications;

Malaysia and Singapore's Personal Data Protection Acts enacted in 2010

# THE BIG COUGH UP

## WHAT'S THE **COST OF LAX DATA CULTURE?**

On 20 September 2018, a UK regulator ordered Equifax, a global credit reporting agency with access to sensitive consumer data used by banks and other creditors to determine customer default rates, to cough up GBP500,000 for one of the biggest data hacks in the financial services sector.

The UK's Information Commissioner's Office (ICO) fined Equifax Ltd. for failure to protect the personal information of up to 15 million Britons. The data breach occurred as part of a wider cyberattack against its American parent company, Equifax Inc., and the loss of personal information – names, dates of birth, addresses, passwords, driving licences, financial details – affected 146 million global citizens between May and July 2017.

The ICO, which carried its investigation in parallel with the Financial Conduct Authority, stated in a press release that Equifax's UK arm failed to take appropriate steps to ensure its US parent, which was processing the data on its behalf, was protecting the information. The investigation was carried out under the Data Protection Act 1998 – the legislation in force at the time of the leak – that has since been replaced with the more stringent GDPR.

The company contravened five out of eight data protection principles, including failure to secure personal data, poor retention practices, and lack of legal basis for international transfers of UK citizens' data.

Prior to the breach, multiple alarms were raised to Equifax, including problems in data retention, IT system patching, audits, and a security warning by the US Department of Homeland Security as far back as March 2017. The corporation swept these under the carpet. Once discovered, it was slow in coming forward to announce the data hack, revealing it only six months after.

The UK Information Commissioner Elizabeth Denham summed it thus: "The loss of personal information, particularly where there is the potential for financial fraud, is not only upsetting to customers, it undermines consumer trust in digital commerce.

"This is compounded when the company is a global firm whose business relies on personal data.

"Many of the people affected would not have been aware the company held their data; learning about the cyberattack would have been unexpected and is likely to have caused particular distress.

"Multinational data companies like Equifax must understand what personal data they hold and take robust steps to protect it. Their boards need to ensure that internal controls and systems work effectively to meet legal requirements and customers' expectations. Equifax Ltd. showed a serious disregard for their customers and the personal information entrusted to them, and that led to today's fine."

Since news of the cyber breach erupted, Equifax has been hit by a rare 50-state class action lawsuits, hundreds of individual class action lawsuits via small claims court, over 60 government investigations from US state attorneys general, federal agencies, and the British and Canadian governments.

At the time of writing, Equifax has said it is still mulling its response to the ICO penalty.

**+ The media often portray data privacy scandals as arising from criminal hackers or collusive behaviour among big organisations. Think Facebook and Cambridge Analytica. But oftentimes, privacy breaches stem from unsophisticated, good ol' human behaviour – theft, loss, or accidental disclosure.**

and 2012 respectively, which regulates the collection, disclosure, and use of client data; and

Australia's Notifiable Data Breaches Scheme introduced on 22 February 2017, requiring government agencies and other entities to notify data owners in the event of a data hack.

## DOXXING DOWN UNDER

The media often portray data privacy scandals as arising from criminal hackers or collusive behaviour among big organisations. Think Facebook and Cambridge Analytica. But oftentimes, privacy breaches stem from unsophisticated, good ol' human behaviour – theft, loss, or accidental disclosure.

To illustrate, Australia recently made headlines when *ABC News* obtained a list of reported privacy breaches by the nation's four largest banks between January 2012 and April 2018. Its investigative news segment, *7.30,* recently invoked freedom of information laws to obtain documents which showed 32 breaches by major banks filed with the Office of the Australian Information Commissioner, including:

- National Australia Bank: An employee involved in a private Facebook dispute with a member of the public took revenge by setting up a fake Facebook identity to reveal the address of the other party. This is known as 'doxxing' or publishing an individual's private information on the internet with malicious intent.
- Westpac: A relationship manager gave the banking passwords of 80 customers to a mortgage broker, whilst in other instances, employees accessed the accounts and transaction information of spouses and other customers, including public personalities. Separately, customers using Westpac's new 'tap and pay' wearable banking software discovered that they were able to see other customers' banking details on their devices.
- An ANZ subsidiary lost a box of files containing customers' financial information, conversation records, and identification documents.


## CULTURE, NOT CODE

The US-based International Association of Privacy Professionals recommends these practical ways to build a strategy and instil a progressive culture when it comes to data privacy.

**STRATEGY 1** Get the basics right. Assess the current state of your privacy programme including privacy policies, breach response protocols, and training. If there is a strong sense that "we don't know what we don't know", completing a privacy gap analysis is a good first step.

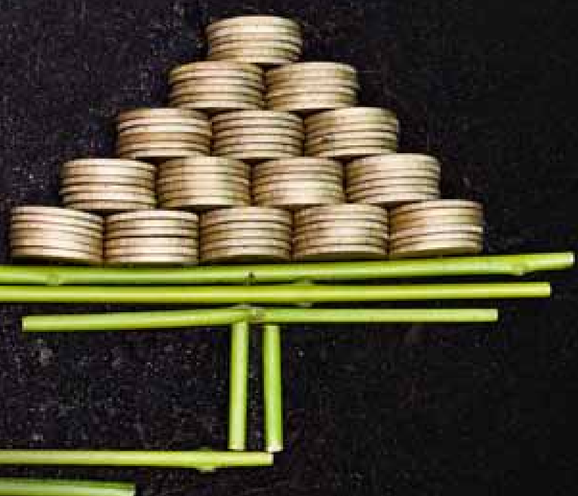
**STRATEGY 2** Align the organisation's privacy programme with its strategy and values. Many leading organisations build the responsibility for protecting data privacy directly into their codes of conduct, requiring employees to formally review and sign off on their understanding of the code every year. For this to work, managers must model the behaviours demanded by the code and instances of employee non-compliance must be dealt with swiftly and consistently.

**STRATEGY 3** Integrate the privacy programme within existing business processes. Define the critical business functions within the organisation. Some of the key integration points are human resources, new business development/ capital project approvals, project management office, risk management, and procurement. ✱

■ *Kannan Agarwal is an assistant researcher currently engaged in economic and financial modelling with a social enterprise.*

BY DR ADAM NG, DR GINANJAR DEWANDARU, RUSLAN NAGAYEV AND ESMA NIZAM

**Currently, sustainability is one of the most significant trends in the industry. It could be in the form of investors' desire for sustainable responsible investing or corporate management's focus on corporate social responsibility or governments' focus on sustainability and environmental impact issues.**



# THE IMPACT OF SOCIAL AND ENVIRONMENTAL SUSTAINABILITY ON FINANCIAL PERFORMANCE

## A GLOBAL ANALYSIS OF THE BANKING SECTOR

New study is **food for thought** for banks, investors, and policymakers.

In today's socially conscious market environment, sustainability trends have altered how businesses run their operations. This is supported by international bodies like the United Nations, Global Reporting Initiative (GRI), Sustainability Accounting Standards Board, World Business Council for Sustainable Development, and Principles for Responsible Investment that have set the principles, guidelines, and best practices for corporations to manage their various functions and assets in a more sustainable multi-stakeholder manner. As such, this trending concept has become the new language of business, whereby firms not only need to sustain their financial strength (for shareholders) but also their social and environmental impacts on the broader stakeholders, namely the community, consumers, customers, suppliers, employees, investors, and regulatory bodies. The broad perspective on organisational value has morphed far beyond the domain of financial and accounting statements.

The banking sector plays an important role in sustainable development. Currently, sustainability is one of the most significant trends in the industry. It could be in the form of investors' desire for sustainable responsible investing or corporate management's focus on corporate social responsibility or governments' focus on sustainability and environmental impact issues. According to Sustainalytics' 2014 *Thematic Research Report,* banks are the heart of all modern markets; they pump financial means like lifeblood through the system, enabling innovation, economic growth, and prosperity. However, the role of financial establishments often goes beyond their original function as intermediaries. It is noted that the core function of banks as enablers of economic growth and prosperity remains undisputed, but civil society, particularly in the developed world, is increasingly concerned about how they fulfil this purpose. Many have expressed the need for 'moral capitalism' that is in tune with social and environmental concerns. Banks have been criticised by civil society groups wanting a large stewardship commitment, regarding their involvement in aiding businesses and development that immensely harm the environment, undermine human rights, and are connected to severe adverse impact on local communities. Although in all these cases financial institutions do not directly affect the society and environment, they have the capability to do so indirectly via their influence on the businesses they finance.

Despite the promising evidence of the corporate social performance–corporate financial performance and corporate environmental performance–corporate financial performance relations across various business sectors, the findings from the banking sector remain limited and inconclusive. Some empirical studies in the banking industry discover a positive link between financial performance of the banks and social performance (Simpson & Kohers, 2002; Cornett et al., 2014), governance (Aebi, Sabato & Schmid, 2012), and environmental-friendly performance (Jo, Kim & Park, 2014). As banks work to restore their credibility following the global financial crisis and contribute to financial stability, timely and strategic integration of sustainability into their businesses remain a crucial agenda for change. Sustainability can be practised from the inside (banks' internal operations) to the outside (banks' financing and investment portfolio, client and community relationships). Nevertheless, other empirical research reveal an opposite evidence: Financial performance has a negative relation (Soana, 2009; Nollet, Filis & Mitrikostas, 2016), or no significant relationship with sustainability business practices (Chih, Chih & Chen, 2010).

This article is an encapsulation of a technical research that seeks to identify and understand the impact of banks' social and environmental performance on their financial performance through (i) identification of the significant or material data or information that may have an impact on the banks' financial performance, (ii) examination of the means through which the social and environmental performance values translate into the banks' financial performance, (iii) assessment of whether social and environmental indicators have a significant impact on the banks' financial performance, and (iv) identification of the threshold of social and environmental impact on the banks' profitability, which may vary depending on bank size and level of social and environmental performance. This study controls for the type of financial institution such as commercial banks, cooperative banks, investment banks, Islamic banks, private banking or asset management companies, real estate and mortgage banks, and savings banks. This study also takes into account both the bank-specific variables and the macroeconomic variables. Finally, this study takes into consideration reliability and comprehensiveness of dataset. We use MSCI (previously merged with KLD) as our source of sustainability data, which is the latest and in-depth social and environmental database used for the reference and datapoint. MSCI data has been widely applied in the literature by researchers and academicians examining the relation between social responsibility and financial performance (e.g. Graves & Waddock, 1994; Turban & Greening, 1997; Mattingly & Berman, 2006; Godfrey, Merrill & Hansen, 2009; Ioannou & Serafeim, 2014). The key justifications, findings, and contributions of the research are elaborated briefly below.

**While banks might understand the relationship between their sustainable performance and business performance, banks need to be able to value map the material social and environmental indicators into business performance with reasonable data availability and quality.**

While banks might understand the relationship between their sustainable performance and business performance, banks need to be able to value map the material social and environmental indicators into business performance with reasonable data availability and quality. This in turn will help investors (including current and future shareholders) integrate their sustainability evaluation

into the decision-making and business processes. An increasing number of investors commit to the integration of social and environmental sustainability in their investment process. However, which of these social and environmental sustainability data should be taken into consideration is still a matter of further exploratory discussion and debate.

The research considered the materiality aspects of social and environmental sustainability affecting financial institutions. Materiality is key in the study of sustainability performance in the banking sector. Without materiality determination, the study would not be able to open the door to measuring sustainability effectively, if not accurately. Therefore, to measure the impact of banks' social and environmental sustainability performance, the study must identify the factors that materially affect banks' performance. This study uses material dataset in assessing the impact of social and environmental sustainability performance on banks' financial performance. This way, the study fills the gap in the existing empirical literature, which mainly uses the non-material dataset.

Secondly, previous studies were not able to identify the channels through which social and environmental

sustainability performances generate positive impact towards the financial performance of the bank. As such, this study expanded the understanding of the relationships among the identified variables in the model and allows more hypotheses to be tested systematically. The analysis using the interaction term suggests that management quality or firm efficiency is one of the channels through which the value from access-to-finance (a key social sustainability component in the banking sector) could flow to business performance of banks. Additionally, loan growth is also identified as another medium to which sustainability value could flow to banks' financial performance. Inclusion of the interactive term in this study helps us to understand how this positive sustainability is being channelled to the business performance of banks.

Thirdly, by applying the threshold regression estimation method suggested by Hansen (2000), we find that there is no statistically significant sample splitting when access to finance is used as a threshold variable. In other words, the varying degrees of access to finance (low, medium, or high) have no effect on the return on equity (ROE) of banks generally. However, there is significant sample split when bank size is used as a threshold variable. Banks with total assets lower than US$2.07 billion experience significantly positive impact of access to finance on their ROE. In essence, smaller banks will have significant impact as compared to larger banks when they partake in providing access to finance initiatives. We find that banks that score below 1.51/10 for environmental financing experience negative impact on their financial performance. This is probably due to the negative environmental impact arising from reputational damage, erosion of collateral value due to environmental damage, increase in litigation and default risk, and potentially regulatory fines. Interestingly, there is no statistically significant effect on banks' financial performance for banks that score above 1.51 in environmental financing, although sign of the coefficient is positive. One plausible explanation could be that banks require time to realise the potential upside of environmental financing as per Jo, Kim & Park (2014) who revealed that reducing environmental costs takes at least one or two years before increasing return on assets. We find that differences in bank size do not matter as environmental financing is not statistically significant in both small and large banks.

Based on this study, market investors and analysts will have a better understanding of social and environmental sustainability and how it affects the firm's performance in general, and banks specifically. This can be used for future valuation of bank's financial and environmental, social, and governance performance, and whether to afford premium or discount accordingly. Therefore, financial institutions are incentivised to graduate from greenwashing or altruism to strategic objectives by incorporating social and environmental sustainability into their business strategy goals and business performance. As investors become more and more sophisticated and aware of the implications of various pieces of financial information towards the future financial performance of a company, stock prices are incorporating this information with greater efficiency and with less bias.

Findings of this study also have bearing and implications toward policy and regulatory development in the banking sector. Policymakers should endeavour to create an institutional environment that is conducive to social and environmental sustainability practices in the financial sector. Ng (2016) highlighted that if allowed to operate in a conducive political and economic environment, coupled with a level playing field and profit-making prospects, the financial sector can be a significant contributor to the economy. To avoid any unintended consequences of counterproductive regulation and to enable an environment that promotes informed policy drafting, banks should consider playing a proactive and collaborative role with regulators and policymakers.

Tiered incentive structures could be explored by policymakers and regulators to encourage small- and medium-sized banks to embrace social and environmental sustainability practices, as opposed to across-the-board requirements. For example, the global standard-setting body for sustainability reporting, GRI, provides their signatories with guidelines and milestones to be achieved within a stipulated time period. Policymakers may also consider incentivising banks and financial institutions to become more pro-environment through measures such as imposition of taxes on environmentally harmful products or services, imposition of a percentage of greenery compulsory in financing development projects, and granting of tax deductions for environmentally friendly activities within communities. ✱

*The authors acknowledge the research grant from Khazanah-INCEIF Research Collaboration on Islamic Finance. Opinions and analysis expressed in this article are solely by the authors.*

■ *Dr Adam Ng, Deputy Director, Research Management Centre, International Centre for Education in Islamic Finance (INCEIF); Dr Ginanjar Dewandaru, Director, BNP Paribas-INCEIF Centre for Islamic Asset and Wealth Management; Ruslan Nagayev, Assistant Professor, Istanbul Sabahattin Zaim University; and Esma Nizam, Vice President, Khazanah Nasional.*

# A New Cyber Framework

New cybersecurity standards are just around the corner. But, asks EMILY PERRYMAN, is regulation the best way to **boost resilience to cyberattacks** and major information technology failure?

A wave of cybersecurity attacks on Britain's leading banks has encouraged the Bank of England's Financial Policy Committee (FPC) to develop a framework that aims to increase resilience to operational risk. Due to come into effect in 2019, the new standards will lay out how quickly the FPC expects firms to restore vital services should they fall victim to a cyberattack. The Committee is also piloting a new stress-testing approach, in conjunction with the National Cyber Security Centre, to ensure firms can meet its standards.

This comes after the Bank of England, the Financial Conduct Authority (FCA), and the Prudential Regulation Authority (PRA) published a joint Discussion Paper on the ability of firms to respond to and recover from cyberattacks, as well as what they can learn from them.

The Discussion Paper has enabled the supervisory authorities to collate their views on how to improve operational resilience, after the PRA announced in April that it intended to develop a set of cybersecurity standards that would apply to the entire financial services sector, including banks, insurers and investment firms.

The increased focus on cyber resilience follows a series of high-profile attacks on seven of the UK's biggest banks in 2017, as well as major technology failures at Visa, TSB Bank and the London Stock Exchange this year. Speaking on behalf of the Bank of England, Lyndon Nelson, Deputy Chief Executive Officer of the PRA, warned that although banks have been safeguarding their financial interests against fraudsters for decades, "in the case of operational matters, the barriers to entry for those who would seek to do harm to the bank are much lower".

## CONTINUITY OF BUSINESS

As yet there is very little detail on what the new framework will encompass. Nelson, however, has said that firms will be expected to: Draw up their own metrics of when an attack would constitute a threat to consumers or financial stability, regularly


**Draw up their own metrics of when an attack would constitute a threat to consumers or financial stability, regularly test their approaches to incidents, and have contingency plans for the resumption of critical functions.**

It's important to have measures that encourage companies to take security seriously, and organisations will already have a range of cybersecurity standards, tools, metrics, and approaches in place. However, as cyber resilience is increasingly incorporated into the overall resilience of an organisation, new standards should view this issue holistically, against the context of the wider organisation, and as organisations become more interdependent.

test their approaches to incidents, and have contingency plans for the resumption of critical functions.

The heightened regulatory focus has been broadly welcomed by the financial sector. "Technology is an enabler for the services that customers and businesses rely on in their day-to-day lives. It is therefore right that the Bank of England has chosen to focus on continuity of business services and the area of operational resilience in more depth," said a spokesperson for the trade association, UK Finance.

"It's important to have measures that encourage companies to take security seriously, and organisations will already have a range of cybersecurity standards, tools, metrics, and approaches in place. However, as cyber resilience is increasingly incorporated into the overall resilience of an organisation, new standards should view this issue holistically, against the context of the wider organisation, and as organisations become more interdependent."

For banks with strong cybersecurity policies already in place, any new regulations may appear an unnecessary additional – and expensive – burden. A poll by corporate adviser Duff & Phelps of 200 financial services firms last year found that 86% were already planning to spend more time and money on cybersecurity, up from less than 60% in 2016.

But Marcus Scott, Chief Operations Officer at TheCityUK, an industry-led body for UK-based financial and related professional services, points out that although there are very high standards of cybersecurity among big firms, this isn't necessarily the case among the smaller ones. "All firms, even the tiny ones, hold important information about individuals which could allow fraudsters to con people out of money," he says.

"The Bank of England can't undertake its CBEST cybersecurity testing with all the small firms, so it needs to develop best practice. At the moment, there is no real consensus in the market of what good practice looks like."

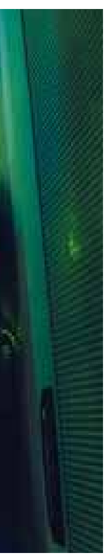
Scott points out that because financial firms are interconnected, it is important for the industry as a whole that smaller firms are encouraged to focus on cyber resilience: "We need to ensure the companies that banks are servicing and lending to aren't the weak link in the system."

## AN EVOLVING PROBLEM

One of the difficulties with cybersecurity, as opposed to other types of business risks, is that criminals' expertise is constantly evolving. "There's a distinction between resilience against systems failing and resilience in the face of external actors who are trying to break you," says David Aspinall, Professor of Software Safety and Security at the University of Edinburgh. "Attackers who are deliberately looking for ways to break the system have an asymmetric advantage because they can be using cheap and plentiful computing resources, they're often spread out around the world, and they're often finding out about software vulnerabilities more quickly than bank information technology systems can be patched."

At the same time, the world's dependence on online financial services is growing exponentially. Internet banking use among British customers, for example, is projected to rise from 53% in 2014 to 66% by 2020, according to the Centre for Economics and

However, during the same period the attackers have also become more sophisticated and powerful and our dependence on online financial services has become more critical," he adds. "Therefore, I conclude that, 'adjusting for inflation', we may be worse off now than we were five years ago as the potential threats and resulting consequences are of a much greater magnitude.



Business Research. This represents an increase of almost 7.5 million internet banking users in just six years.

Ashley Stephenson, Chief Executive of software company Corero Network Security, says that in the past five years banks have come a long way in the context of cybersecurity. They are better informed, better prepared and more likely to disclose a cyberattack. "However, during the same period the attackers have also become more sophisticated and powerful and our dependence on online financial services has become more critical," he adds. "Therefore, I conclude that, 'adjusting for inflation', we may be worse off now than we were five years ago as the potential threats and resulting consequences are of a much greater magnitude.

"This means that in the context of cyber risk, the sector must continue its efforts to share information, boost its goals for cyber resilience, deploy active cyber protection and welcome, rather than resist, efforts to increase cyber regulation."

## PRINCIPLES AND OUTCOMES

With cybercriminals becoming increasingly advanced and skilful, it is hoped the FPC is not overly prescriptive when developing its standards. UK Finance says it is important to have regulation that is responsive to the changing risks that organisations and services face. "This could mean a principles-based approach, rather than point-in-time regulations that just meet the needs of today's operative environment," says the organisation's spokesperson.

Scott suggests the standards will adopt the outcomes-based approach that regulators such as the FCA have applied to other types of financial regulation. "Rather than specifying what individual technology a firm requires, the standards are more likely to focus on the behaviours and attitudes of companies," he explains. "If the standards are simply a tick-box exercise, cybercriminals will very easily find a way around them."

Diversity of implementation is thought to be an important tool against cyberattackers. "Drawing an analogy with physical security, if every bank has the same lock, there is compelling motivation for the bad guys to find the master key. A similar situation exists for cybersecurity: If exploiting a vulnerability at one bank exposes many more institutions that are using the same defence solution, the results are potentially catastrophic," warns Stephenson.

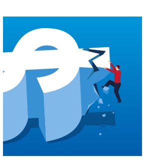
## WATCH THIS SPACE

With several months still to go before the new framework comes into effect, for banks it is very much 'watch this space'. One thing is for sure, though: Cyberattacks are now a constant threat for the financial sector and are likely to be a key regulatory focus in the years to come. The framework will hopefully encourage the development of systems and procedures that better protect both banks and their customers. ✱

■ *This article was previously published in the Chartered Banker Magazine, October/November 2018.*

# GREAT TO GOOD

Innovations of the 21st century are breaking the mould and doing more with less.



**+ Management consultant giant, McKinsey and Company, did a follow-on study that found 32 of the 50 companies described in these books had only matched or underperformed the market in the subsequent 15-to-20-year period. In fact, the 'great' Circuit City and Kodak both went bankrupt.**

Yes, you read it right. The title of this piece is *Great to Good.* I'm going to talk about how, in the 21st century, we need 'goodness' more than 'greatness' when it comes to innovation.

Between 1996–2001, Jim Collins' team researched and wrote a bestselling book called *Good to Great.* They described 11 out of 1,435 companies that had shown the highest levels of success over decades. Most of them were organisations that 'make and sell' products, such as Abbott Laboratories, Kimberly-Clark, Philip Morris, and Gillette. Other books such as *Built to Last* (1994) by the same author and *In Search of Excellence* (1982) by Tom Peters made similar studies with concurring results.

However, the majority of these great 20 th century companies failed to sustain their level of greatness in the Open Source era. Management consultant giant, McKinsey and Company, did a follow-on study that found 32 of the 50 companies described in these books had only matched or underperformed the market in the subsequent 15-to-20-year

The answer, to me, is how the meaning of innovation has changed. We have spent over a century making and producing 'things'. Never has the world experienced so much wealth, consumed so much resources, collected so much assets, and generated so much waste.

period. In fact, the 'great' Circuit City and Kodak both went bankrupt.

The question is "Why?"

If I asked you to name some innovations of the 20th century, which ones would you think of? Well, many of you might already be thinking, "Stop asking and just Google it, silly!" That is true, excuse me. So I typed "innovations of the 20th century" and the results I got were: (1) nuclear power, (2) personal computer, (3) airplane, (4) automobile, (5) antibiotics, (6) television, etc. We are familiar with all these inventions.

Here is another question: Do you know who these people are and what they invented? In parentheses are their dates of birth: Thomas Edison (1879), Albert Einstein (1921), Alexander Fleming (1928), Edwin Land (1948), Robert Metcalfe (1973), and Peter Dunn and Albert Wood (1998)?

They are inventors from the 20th century, many of whom gave rise to the said products.

Now, how about these names?

Jack Ma (2000), Jeff Bezos (2003), Mark Zuckerberg (2004), Reed Hastings (2007), Brian Chesky (2008), Travis Kalanick (2009), and Anthony Tan (2012). They are also inventors, but from the 21st century.

Obviously, all names listed are innovators of their time. But the real question is, what is the difference between the first and second sets?

The answer, to me, is how the meaning of innovation has changed. We have spent over a century making and producing 'things'. Never has the world experienced so much wealth, consumed so much resources, collected so much assets, and generated so much waste. In fact, most of us own at least four of the six

Innovations of the 21st century do not rely on one to discover the secret codes of the universe. Facebook basically lets people around the world share their diaries, Airbnb is a brokerage for vacant rooms, and Grab is a virtual concierge that gets us a cab. There is no complex ingenuity at play here, only laymen who see questions the world has been waiting for answers to.

examples of innovation of the 20th century that I have outlined above. Books such as *Consumptionomics: Asia's Role in Reshaping Capitalism and Saving the Planet* by Chandran Nair, and *Abundance: The Future is Better Than You Think* by Peter H. Diamandis and Steven Kotler, provide further evidence of this prosperity.

By the way, in case you were wondering, Peter Dunn and Albert Wood are inventors of the performance-enhancing drug, Viagra.

Innovation in the 21st century, however, is about sharing – not producing. If I were to now Google "innovations of the 21st century", here is what it would tell me about inventions that are impacting lives: "The world's largest taxi firm, Uber, owns no cars. The world's most popular media company, Facebook, creates no content. The world's most valuable retailer, Alibaba, carries no stock. And the world's largest accommodation provider, Airbnb, owns no property. Something big is going on."

These businesses own virtually nothing of what they provide to customers, yet they have created tremendous value and change in the world. Unicorns, decacorns and hectocorns are the theme of the present era. It is the age of making money out of nothing, what Hamish McRae (@TheIndyBusiness) dubbed "the rise of content non-generator". As a matter of fact, businesses of the 21st century are being invested based on their 'value-ation' rather than the traditional return on asset or profit and loss statements.

Even Google does not own the search results that are returned. It merely draws it from existing data generated by millions of resources around the world.

The innovations of the 21st century are different. Something big is indeed going on.

The 20th century was an era of geniuses. One need not ponder long to think of Albert Einstein, the inventor of the E = mc2 equation, the theory of relativity, and a recipient of the Nobel Prize for discovery of the photoelectric effect, which serves as the basis for quantum physics. Or even before that, we had Thomas Edison, a prolific inventor with 1,093 US patents in his name. These genius discoveries have since given birth to products like nuclear power, lights, television, automobile, spacecraft, etc. Such influence partly explains why most parents strive to raise their kids to be as smart as possible. The genius craze led to children books with titles like *Raising Genius,* the *Baby Genius* DVDs, and movies such as *Good Will Hunting,* starring Matt Damon as the improbable 'genius'.

Notice that none of the innovators in my second list have a Nobel Prize. And I think it is unlikely that any of them will ever be given one.

Innovations of the 21st century do not rely on one to discover the secret codes of the universe. Facebook basically lets people around the world share their diaries, Airbnb is a brokerage for vacant rooms, and Grab is a virtual concierge that gets us a cab. There is no complex ingenuity at play here, only laymen who see questions the world has been waiting for answers to. These start-ups simply integrate and utilise things that already exist to provide good answers. In the current era of resource abundance, one does not need to have an IQ of Einstein or dedicate one's life to failing 10,000 times like Edison to concoct an invention. A good idea or two will suffice.

The 20th century was about a few people finding GREAT discoveries. The 21st century is about all of us, using the breakneck-speed connectivity that technology provides, to do GOOD things

The 20th century was about a few people finding GREAT discoveries. The 21st century is about all of us, using the breakneck-speed connectivity that technology provides, to do GOOD things together for a better future. That is my meaning of *Great to Good.*

together for a better future. That is my meaning of *Great to Good*.

**LEADERSHIP INSIGHTS**

**The New S Curve:** Organisations in various countries that I work with are all buzzing about disruptive innovation – how to build the new growth cycle. To begin cracking that code, one must understand that innovations of this era are unlike anything we have ever seen before. I would argue that even iPads, iPhones, electric cars, or robotics are all innovations of the previous era, with substantial improvement made by the evolution of technologies. On the other hand, innovations of the 21st century are about connecting, linking, integrating, and creating a better future. They are not addressed by appointing a research-and-development team, integrating the best of tech, stretching product development to design new models and services, or even hiring great talent. The crux of innovation in this very age is about taking what already exists and synergising new values out of it. Only by shifting how your people think about innovation and letting the cream rise to the top will you achieve such breakthrough leadership.

**Criteria for Innovation in the 21st Century:** Rachel Botsman and Roo Rogers, authors of *What's Mine Is Yours: The Rise of Collaborative Consumption* (2010), described key components of these 'sharing' innovations:

- i ***Critical Mass:*** Reaching target groups with massive number of people. This is the reason why Amazon.com, Alibaba, and Uber endured years of losses in order to build their networks.
- ii ***Idling Capacity:*** Noticing the existing resource that can be utilised. For example, AirAsia allow passengers to print their own boarding pass from home; banks let customers carry out transactions via the internet; and Airbnb uncover the unoccupied spaces in the community and unleash them for rent.
- iii ***Common Base:*** Willingness to share interests, knowledge, and capabilities between peers. This happens when we share our life stories on Facebook, rely on HappyFresh workers to buy our grocery for us, or report a crash on Waze to benefit other drivers.
- iv ***Trust Creation:*** The system for building peer groups. For example, the Grab app entrusts us to get into a stranger's car because we are comforted by the 'stars' given.

**The Time is Now:** This golden opportunity of the 21st century is literally up for grabs (pun intended). We are now living in an era where innovations are not limited to selective people with genius IQ. Thus, be diligent in your search for new knowledge, be brave in challenging the boundaries of what you know, and find a simple yet unresolved problem that has been making you sad or angry. Then, put on your leadership hat. Think about how this problem also affects other people like you. What might be a pent-up resource that could be released to address this challenge? Will people be open to putting in their own efforts and spread the growth? Finally, identify what connectors must be made to build trust and pave the way for a society of sharing.

Welcome to 'great to good' innovation. Strive for 'goodness' as opposed to 'greatness'. And let's make our world a better place. ✱

■ *Dr. Thun Thamrongnawasawat is Director of Research and Curriculum at the Iclif Leadership and Governance Centre.*

# Call of Duty

RULES ARE NOT THE PANACEA FOR UNETHICAL BEHAVIOUR. IT'S NECESSARY ALSO TO **DEFINE THE UNIVERSAL AND INCONTESTABLE DUTIES** OF THE BANKER.

For the last ten years, financial institutions have been working desperately hard to rebuild the trust and confidence of their stakeholders after the seismic events of the global financial crisis. Governments, regulators, even directors and executives of the banks themselves all agreed that change for the better would not just happen on its own, but would have to be driven.

It is now generally accepted that a new, more ethical banking climate relies greatly on acknowledgement of duties. There has been much discussion about how to achieve the appropriate 'tone at the top' and the need to embed the interests of customers and other stakeholders at the heart of everything the bank does. As the majority of banks are joint-stock companies, their primary duty is to maximise shareholder value, but it is clear that this can only be done in a financially sustainable manner by pursuing policies that pay due regard to the interests of customers, employees, the community and even the physical environment. This idea, sometimes referred to as 'enlightened shareholder value', implies that banks need to extend their fiduciary reach beyond customer satisfaction alone.

**It is now generally accepted that a new, more ethical banking climate relies greatly on acknowledgement of duties.**

Can the duties of banks be codified in some way, and if so, can these codes be used as the basis for transformation? Certainly some banks think so, as it is now unusual to find a bank which does not have some sort of code of practice, code of ethics or other statement of social responsibility. This is probably the most productive approach, because it became quite clear that rules were not a cure-all, especially as some of the most rules-laden systems in the world suffered the same or even more severe problems than less rules-driven systems when the crisis hit them hard. In fact, most professionals are driven by principles, and know that if they adhere to the universally acknowledged standards of honesty and probity, there is less need to rely on copious sets of rules.

The duty-based approach to securing ethical behaviour is built on sound foundations. In the late eighteenth century, Immanuel Kant formulated his concepts of hypothetical imperatives and categorical imperatives as elements of his deontological (duty-based) theories.

A hypothetical imperative arises when a specified action is required to achieve a defined result. In this way, we understand that to become good athletes we have to keep fit and push physical boundaries. To achieve professional competence, we have to study and learn from our experiences.

By contrast, a categorical imperative is an absolute requirement which should apply all the time, regardless of circumstances. When considered in the context of duties of individuals to do right as opposed to wrong, Kant argues that there are universal principles that must apply as ends in themselves. Central to this notion is his statement, "Act only according to that maxim whereby you can, at the same time, will that it should become a universal law". This is not far removed from the so-called 'golden rule' accepted in many religious sources:

> "Pay, O Children of Adam, as you would love to be paid, and be just as you would love to have justice." *(Quran, 83:1–6)*
>
> "Do unto others as you would have them do unto you." *(Bible, Matthew 7:12 and Luke 6:31)*
>
> "Those acts that you consider good when done to you, do those to others, none else." *(Shikshavalli, Eleventh Anuvaka)*

It would appear to be relatively easy to come up with a set of duties or universally applicable principles in the context of banking, and in turn use these to guide professional bankers towards good behaviour and hence positive outcomes. These are often set down as fundamental ethical principles such as honesty, probity, integrity, transparency and so on. However, a problem arises when we discover that our ostensible categorical imperative is not actually categorical at all. Take for example the view that it is wrong to steal. Most people would agree that it is always wrong to steal. However, British philosopher R.M. Hare cited the example of an individual who finds a set of plans belonging to a terrorist who wants to commit an atrocity at the cost of many innocent lives. Surely it is not wrong to steal those plans?

Likewise, we can see other 'exceptions to the rules':

Counter staff should always tell the truth (or should not tell lies), but they may have to tell a lie when faced with a suspicious transaction if the customer is not to be 'tipped off'.

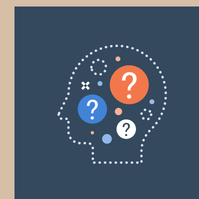
Banks should be transparent, but it may not always be possible to give a customer complete information on a new product that will be better for them until the product is in the public domain.

Banks should respect the confidentiality of customers, but there are exceptions to this too, such as when disclosure is necessary to protect the public interest.

These arguments imply that to every principle it is possible to come up with exceptions, but it does not actually mean that defining duties in terms of universal principles is impossible. In particular, there are three duties which are universal and incontestable.

Firstly, nearly every authority agrees that the 'bottom line' requirement for ethical behaviour is compliance with the law. In other words, most would accept that if an individual does not comply with the law, or explicitly breaks the law, that in itself is unethical. However, herein there are two problems: Not all legal acts are ethical purely on the basis that they are compliant with the law; and it is also possible to obey the 'letter of the law' while paying little respect to the intention (or 'spirit') of the law.

Secondly, ethical behaviour is dependent on fairness. This requires the individual and the organisation to act in an even-handed manner, without prejudicing the interests of those with whom they deal. The late Dame Anita Roddick, the founder of 'The Body Shop', was fond of telling the story of her experience when applying for a loan to start her business. She approached a branch office in Brighton (UK), equipped with her business plan and other information, and her application was declined. She then went to a branch of the same bank in Worthing (20 km away), requesting an identical loan and supporting her application with identical information, and the loan was sanctioned. The only difference is that for the first interview she attended in a T-shirt, jeans and training shoes, while for the second interview she dressed formally. This is hardly likely to happen in the 21st century, but it does demonstrate how prevailing attitudes can shape behaviours and decisions.



**Firstly, nearly every authority agrees that the 'bottom line' requirement for ethical behaviour is compliance with the law. In other words, most would accept that if an individual does not comply with the law, or explicitly breaks the law, that in itself is unethical.**

Thirdly and lastly, ethical behaviour is dependent on honesty and good faith. Most banking relationships are contractual in nature. If we accept that it is right to breach a contract, then the whole basis upon which stakeholder relationships are formed breaks down. Conversely, if a bank lends money in the full knowledge that the customer will not be able to service the debt, but does so purely to make a profit, one can imagine the effect this would have if applied universally. To those who have studied the causes and effects of the US sub-prime crisis and subsequent property market collapse, this should be uncomfortably familiar. ✱

■ *Robert (Bob) Souster is a Partner in Spruce Lodge Training, a consultancy firm based in Northampton, England. He lectures on economics, corporate and business law, management, corporate governance and ethics. He is the Module Director for 'Professionalism, Regulation and Ethics', a core module of the Chartered Banker MBA programme at Bangor University, Wales.*

# Raise the Curtain

## WOMEN & FINANCIAL AUTONOMY

It's time banks up their game for the **millions of unbanked women** and close the financial inclusion gender gap.

The business case for providing women with greater access to financial services has never been clearer.

In Asia Pacific, McKinsey Global Institute's recent report, *The Power of Parity: Advancing Women's Equality in Asia-Pacific*, predicts GDP could increase by US$4.5 trillion in 2025 by advancing women's equality, a 12% increase over business-as-usual projections.

A Pew Research Center analysis shows that women comprise 40% of the workforce in 80 countries, marking their rise as a growing economic force for financial services. *Harvard Business Review* also cites that women control more than US$20 trillion in annual consumer spending, a figure that's expected to rise to almost US$28 trillion in the next five years.

Yet, that's only part of the story.

**A HOUSE DIVIDED**

In emerging economies, 1 billion out of the 1.7 billion unbanked adults are women who have no access to formal financial services. On owning a bank account, women continue to trail men by seven percentage points, unchanged since 2011. Access to credit is also unequal: Approximately 80% of women-owned small- and micro-enterprises are denied the finance they need, estimated at US$1.7 trillion globally by the International Finance Corporation.

This disparity in financial access between men and women – termed the 'financial inclusion gender gap' – may be the biggest stumbling block in achieving the World Bank's target of universal financial access by 2020.

The Global Financial Inclusion database – the go-to resource on where the world stands for access to basic financial services – noted that while the financial inclusion income gap (which includes men and women) reduced by several percentage points from 2011 to 2014, the global financial inclusion gender gap remained essentially static during the same period.

This means that despite greater global access to financial services, a large proportion of it failed to reach under-resourced women.

This is significant because, as *cliché* as it sounds, money makes the world go round, but more so for women on the fringe of society, whose lack of access to financial services increases their risk of failure or falling into poverty, disempowers them from making independent choices, and stops them from becoming fully engaged in measurable and productive economic activity.

Additionally, Global Banking Alliance

for Women evidenced that bridging the gender gap is a significant market opportunity for finance providers as it yields multiplier effects: Women tend to save more relative to their total income than men, repay loans at a higher rate, buy more products per capita, and be more loyal to their bank if they are satisfied with the customer service environment.

## INCLUSIVE BY DESIGN

The Brookings Institution's *2017 Financial and Digital Inclusion Project Report* categorically states that "full financial inclusion cannot be achieved without addressing the financial inclusion gender gap and accounting for diverse cultural contexts with respect to financial services".

But closing the financial inclusion gender gap will only happen when financial institutions *en masse* view and treat women as a distinct market segment, collect sex-disaggregated data on their portfolios, and use that data to design products for women clients.

**+ The Washington, D.C.-based think tank lists these action items that may help to reduce the gender gap:**

- advance data collection efforts to determine how groups utilise existing services and identify gaps in the market;
- leverage such data to develop specific targets, initiatives, and strategies for advancing women's financial inclusion;
- identify and cultivate 'champions' to amplify awareness among government entities and private sector representatives regarding gender disparities in financial inclusion;
- promote the development of digital identity programmes;
- leverage digital channels to advance convenient access to financial services; and
- consider how to best ensure customers are comfortable accessing financial services.

But there are also regional variations. In economies like Thailand, there is virtually no gender gap in bank account penetration; whilst in economies like Jordan and Pakistan, women are 50% less likely than men to have a bank account. Much of this discrepancy has a direct correlation to the freedom and rights of women in each country. Thus, if effective solutions are to be devised, country- or regional-specific human rights must be taken into consideration.

## MAKING ACCESS REAL

In recent times, key stakeholders, including financial service providers, rule-makers, policymakers, civil society, and consumers, have explored how best to do this.

Many central banks, especially since 2008, have sought to create a more enabling macroeconomic environment by stimulating real economic activity with a focus on protecting jobs, a marked shift from conventional monetary policy that focus on inflation. In fiscal policies, some governments have implemented gender-sensitive social protection and services by enforcing tax obligations and include gender responsive budgeting in its arsenal of economic tools.

In the private sector, one strategy that has gained immense currency is the deployment of digital technology to boost women's participation in financial services (see box story on the following page), undoubtedly riding the wave of innovation that's risen from the collaboration between fintech and banking proper.

## TAKEAWAYS

Why then hasn't the gender gap in financial inclusion budged since 2008? Does the average woman feel its benefits? Is the needle inching when it should instead be sweeping its way to progress given the immense resources that have been ploughed into the sector?

Banks can seize much more if they customised products and services for women of various demographics, in all settings (rural or urban) and at all levels of business (small, medium, and corporate).

If we want to see catalytic change, governments, the financial services industry, and society must acknowledge that the financial inclusion gender gap is intertwined with our economic reality and their exclusion holds real consequences, financial or otherwise.

Abraham Lincoln, who brought about the emancipation of slaves in America, said, "A house divided against itself cannot stand".

In a world where women comprise 50% of the population, bringing all women into the financial fold unites a house so it cannot fall.

# Bridge the Gender Gap

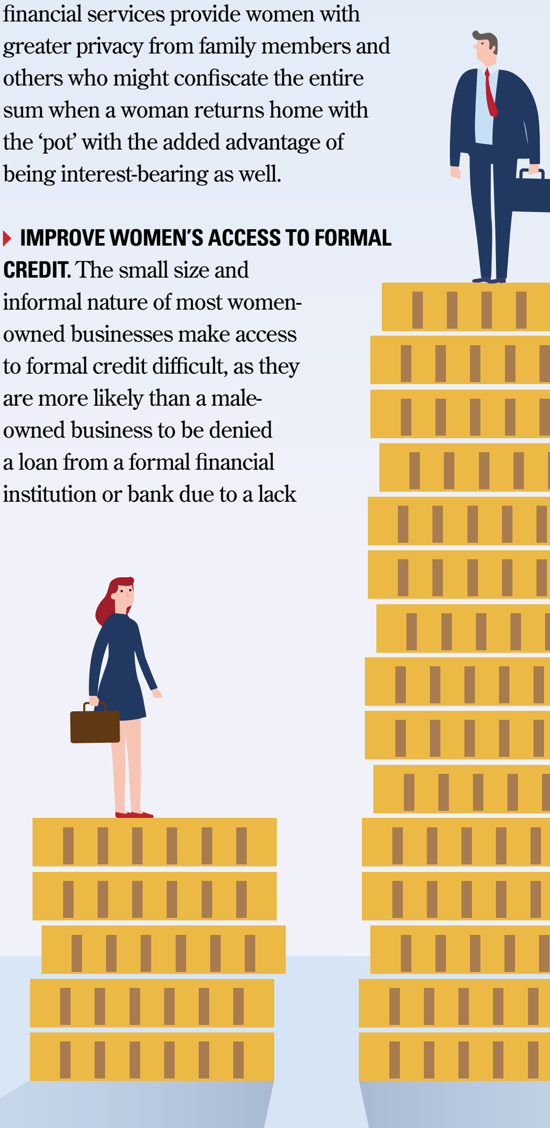
IN 2015, THE GLOBAL PARTNERSHIP FOR FINANCIAL INCLUSION – AN INCLUSIVE PLATFORM FOR ALL G20 COUNTRIES, INTERESTED NON-G20 COUNTRIES, AND RELEVANT STAKEHOLDERS TO CARRY FORWARD WORK ON FINANCIAL INCLUSION – PUBLISHED AN EXTENSIVE STUDY TITLED *DIGITAL FINANCIAL SOLUTIONS TO ADVANCE WOMEN'S ECONOMIC PARTICIPATION,* OUTLINING GLOBAL EXPERIENCES THAT HAVE WORKED FOR THE SECTOR:

- **BRIDGE THE GENDER GAP IN ACCOUNT OWNERSHIP AND INCREASE WOMEN'S PARTICIPATION IN THE FINANCIAL SYSTEM, BOTH IN TERMS OF THE VOLUME AND VALUE OF TRANSACTIONS.** Evidence consistently shows positive economic outcomes for women who access personal savings through their own account, including increased productivity of rural women, increased profits leading to greater business reinvestment, better cash flow to withstand shocks and emergencies, improved consumption smoothing, and greater legal and psychological control over their funds. The frequency and value of financial activity is also positively associated with accessible and affordable digital financial services such as mobile money accounts. Due to cultural norms, family responsibilities, or lower wages, women may be less able to travel to the closest bank branch or meet minimum balance requirements. Encouraging the active use of a variety of financial services – formal savings accounts and loans, insurance, debit cards – can be an effective way to lower the digital gender gap.

- **PROVIDE WOMEN WITH GREATER PRIVACY, CONFIDENTIALITY, AND CONTROL OVER THEIR FINANCES.** With digital transfers, money is sent directly into a woman's account, and the amount and timing are private information. Their savings, salary, or daily wages can be deposited directly into their digital wallets on a daily basis and stored digitally. It might become harder for demanding family members and friends to access information related to these financial transactions. This gives women greater control over how money that is received and/or stored digitally is spent – and they can reinvest that money based on their needs.

- **GIVE WOMEN THE OPPORTUNITY TO SAVE FORMALLY, LOWERING, OR ELIMINATING THE HIGH COST ASSOCIATED WITH SAVING INFORMALLY.** Compared with informal savings schemes, e.g. rotating savings and credit associations which may carry high negative returns due to hidden transaction costs, digital financial services provide women with greater privacy from family members and others who might confiscate the entire sum when a woman returns home with the 'pot' with the added advantage of being interest-bearing as well.

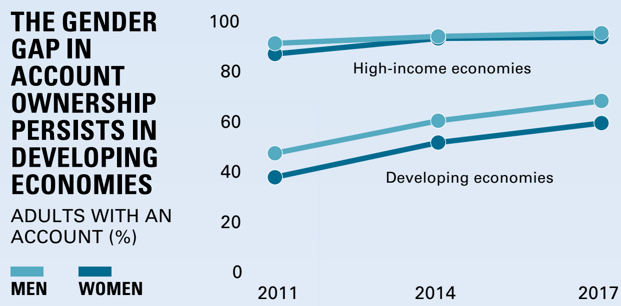
- **IMPROVE WOMEN'S ACCESS TO FORMAL CREDIT.** The small size and informal nature of most women-owned businesses make access to formal credit difficult, as they are more likely than a male-owned business to be denied a loan from a formal financial institution or bank due to a lack



of credit history, collateral, and business experience which are considerations in the credit evaluation process. As banking evolves, building more women-centric products by adopting different metrics for small women-owned business should be part of the equation. Digital platforms also offer the ability to structure new products in a way that could reduce repayment risks, such as microinsurance.

**THE GENDER GAP IN ACCOUNT OWNERSHIP PERSISTS IN DEVELOPING ECONOMIES**

ADULTS WITH AN ACCOUNT (%)




**SOURCE** Global Findex database

**REDUCE TIME SPENT ON TRAVELLING TO ACCESS BANKS OR MAKE UTILITY PAYMENTS.** By providing a digital platform to pay fees and conduct business-related activities, women can free up time to spend on paid work. It can also improve their labour force participation, allow female entrepreneurs to connect with the marketplace virtually, and interact with customers and vendors from the safety of their homes or offices. In addition, women can join firms that allow them to work remotely and get paid through digital channels.

**SUPPORT RISK MANAGEMENT. DIGITAL PAYMENTS HAVE REDUCED RISKS LIKE 'LEAKY' MONEY TRANSFERS, DELAYS, HIGH TRANSACTION COSTS, AND PERSONAL SAFETY.** For instance, in agriculture, some African banks have seen an increase in adoption rates by female farmers for digital insurance products, such as microinsurance against drought or excessive rain, resulting in higher average yields and better managed income shocks. In the US, the federally mandated Electronic Benefits Transfer programme – a digital, debit card-based system – was associated with a significant decrease in the overall crime rate and incidences of robbery, burglary, assault, and larceny, as women who previously kept cash on premises experienced lower risk of theft and harassment. Formal financial institutions also offer electronic records that help deter malpractice and can be used to identify bias/discrimination against women-owned firms.

**IMPROVE WOMEN-OWNED BUSINESSES' ABILITY TO LOWER BANKING COSTS.** Female entrepreneurs – who often run smaller businesses – experience lower profitability because of high account transaction costs, such as account opening fees, minimum balances, transaction fees, etc. Empirical evidence shows that subsidising the cost of maintaining a traditional bank account has a significant positive impact on the adoption of savings accounts among women. To illustrate, when Pakistan's Easypaisa, a branchless banking service, eliminated all fees for account holders for person-to-person (P2P) and a limited number of cash-out transactions, the number of active account holders and the volume of P2P transactions increased.

**HELP FEMALE ENTREPRENEURS BETTER MANAGE THEIR INVENTORY STOCK AND MAKE MORE EFFICIENT PROCUREMENT DECISIONS.** Digital records also can increase small businesses' productivity by lowering costs associated with inventory management. In addition, small businesses can make digital payments to suppliers more frequently, thus shortening the number of days of extended trade credit and lowering working capital expenses.

**HAVE A MULTIPLIER EFFECT THAT DRIVES ADOPTION AMONG MORE WOMEN.** Many women-owned SMEs cater to women's needs. They also hire more women in senior management. By using digital financial tools to collect customer payments and pay salaries, female entrepreneurs may increase digital financial services adoption more broadly among their female employees and consumers, creating a virtuous circle. ✱

 BY PHILIP TE

Breaking Down Barriers: New Mental Models in Risk Management (Lessons Learned from Charlie Munger)

Standfirst <Risk practitioners should explore and inspiration from leaders outside of their industry.>

I teach a course on bank risk management (BRM) based on the two-volume book I have written for the Asian Institute of Chartered Bankers and Oxford University Press. The idea for the BRM qualification came about as a response against too much specialisation in the risk management profession. In all the classes I have conducted for BRM (and my other risk management courses), my conviction is a major risk for banks that must be resolved decisively.

Gillian Tett, US managing editor and columnist at Financial Times wrote an excellent book entitled The Silo Effect: The Peril of Expertise and the Promise of Breaking Down Barriers. In this book, the anthropology-trained columnist wrote of how banks had morphed into gigantic organisations with hundreds of departments or silos that made it impossible for risk managers to access information and understand the complex nature of banking risks. Risk management has become too specialised that risk managers have developed tunnel vision, viewing problems only from their specialised function perspectives. Even the risk models, jargons and measurement tools we use are so fragmented that it is hard to form a unified and integrated view of risk management.

Regulators and policymakers recognised the dangers of these silos in risk management and focused efforts to reduce these organisational silos. In the proposed enhancements to the Basel II framework, the Basel Committee on Banking Supervision (BCBS) stated: "In order to develop an integrated firm-wide perspective on risk, senior management must overcome organisational silos between business lines and share information on market developments, risks and risk mitigation techniques".

New Mental Models From Charlie Munger

While the BRM certification is a step in the right direction, I felt that the traditional mental models we used for risk management should be supplemented with different sets of mental models. I began to seek for these mental models that would allow us to learn from the lessons of past financial crises.

I found the answer in the works of an unlikely person – Charles (Charlie) T. Munger. Munger is the Vice Chairman of Berkshire Hathaway and long-time partner of Warren Buffett. Munger ranks, alongside Buffett, as one of the most successful investors of all time. For decades, value investing practitioners benefited from Munger's investing and worldly wisdom. Munger has spoken extensively on mental models that could improve risk management thinking and behaviour.

In this article, I will discuss three important mental models, which have some direct applications in risk management.

These mental models are:

- invert, always invert;
- multidisciplinary thinking; and
- library of mistakes.

Mental Model 1: Invert, Always Invert

One of my favourite Munger mental models is 'inversion'.

According to Li Lu, a close associate of Munger: "When Charlie thinks about things, he starts by inverting. To understand how to be happy in life, Charlie will study how to make life miserable; to examine how a business becomes big and strong, Charlie first studies how businesses decline and die".

In 1986, Munger was invited to deliver the commencement address at his youngest son's graduation at Harvard University. He deviated from the tradition of providing life advice on how to be successful. Instead, he delivered a long but insightful speech on things that can guarantee a life of misery.

This is a very powerful tool for thinking. According to Munger, some problems cannot be solved forward and should be approached by thinking backwards. He cites Carl Gustav Jacob Jacobi who famously said: "Invert, always invert".

The Number that Killed Us

In solving risk management problems, we frequently try to solve problems forward. Take for instance, the development of the most commonly used market risk model: Value-at-Risk (VAR). It started when Sir Dennis Weatherstone – the former CEO and Chairman of J.P. Morgan – wanted to have a report by 4.15 p.m. summarising the complex market risk exposures of dozens of trading groups within the bank into one, single dollar amount by close of trading day. This has been celebrated as one of the most important milestones in the area of risk management and its use has become pervasive especially in the area of market risk.

Then, the 2008 financial crisis happened. VAR proved to be a tool that did not serve its purpose, especially when it mattered the most. Nassim Taleb, author of Black Swan and Fooled by Randomness, appeared before US Congress and pointed to VAR as the culprit. Taleb, in an interview with Derivatives Strategy in 1996, voiced his criticisms against VAR: "VAR has made us replace about 2,500 years of market experience with a covariance matrix that is still at its infancy…After VAR, all we see is numbers, numbers that depend on strong assumptions".

Had we applied Munger's inversion thinking, instead of approaching the market risk measurement problem in a linearly forward fashion and be satisfied once we see a single dollar amount, we could have inverted and asked the question: "When will VAR fail?" This would have allowed us to uncover the limitations of this risk model and understand deeply the strong assumptions we make in using this model.

Stress Testing and Reverse Stress Testing

Another application I can think of is in the area of stress testing. Stress testing is an important risk management tool used to uncover adverse unexpected outcome. After the collapse of the legendary hedge fund Long-Term Capital Management, which was supposed to be the mother of all hedge funds with proprietors such as the legendary trader John Meriwether (of Liar's Poker fame) and Nobel Laureates Robert Merton and Myron Scholes (from whom the widely used Black-Scholes-Merton formula for option pricing was named), the dangers of using rigid risk models that only work under normal market conditions must be supplemented with a more flexible risk measurement methodology such as stress testing.

The problem with stress testing is you solve the problem forward. Stress testing involves estimating the amount of capital needed to withstand unexpected outcomes. These unexpected outcomes could be based on historical or hypothetical events. This, of course, would be limited by history or by what the mind can conceive as plausible. In short, stress testing usually starts with events (historical or hypothetical) and ends with outcomes (e.g. adverse impact on capital).

Applying the inversion mental model, we could instead attempt to solve the problem backward. Instead of starting with events, we start with a known outcome. We estimate the adverse outcome that could impact our ability to continue to operate as a going concern, then investigate which events could lead to such an outcome. This process is what the BCBS refer to as reverse stress testing. Reverse stress testing helps uncover hidden risks and interactions among these risks.

Mental Model 2: Multidisciplinary Thinking

The 2008 financial crisis created an industry of risk management bashing. In particular, popular literature has heavily criticised the use of quantitative models in risk management and measurement. The mathematisation of finance and risk management models has been heavily and publicly mocked. Massachusetts Institute of Technology Professor Andrew Lo referred to this phenomenon as 'physics envy'. Physics envy has created a false sense of precision and comfort.

Probabilistic Solution to a Deterministic Problem

Taleb criticised our almost religious reliance on risk management, particularly in using probabilistic models to solve a deterministic problem. It's like "crossing a river if it is four feet deep on average". An analogy can be made to bringing 50% of an umbrella because there is only 50% chance of rain.

Munger said: "To a man with a hammer, everything looks like a nail". Munger cautioned everyone not to rely on any single model. Instead, everyone should have multiple models to avoid "torturing reality so that it fits your models".

Munger said: "You must know the big ideas in the big disciplines, and use them routinely – all of them, not just a few. Most people are trained in one model – economics, for example – and try to solve all problems in one way".

He talked about holding a latticework of mental models in the head and "see the relatedness and the effects from the relatedness".

Scenario Analysis: A Triumph in Multidisciplinary Thinking

How do we apply this in the field of risk management? First is to learn from other industries on how they approach risk management. Frequently, we only look at our own industry's unique risks and experience.

However, frequently, we ignore valuable experiences and learnings from other industries that may not have the same risks but have exportable lessons and tools we can learn from.

One example that comes to my mind is the political risks and oil spills by multinational oil companies such as Royal Dutch Shell (Shell). They face material, unpredictable non-financial risks that could have material impact on their business operations.

A visionary Shell French executive, Pierre Wack, pioneered the use of scenario analysis for strategic planning and risk management. This then revolutionary and sophisticated use of scenario analysis prepared Shell through many crises affecting oil prices.

Wack argued that the solution is not to come up with better forecasts but to "accept uncertainty, understand it, and make it part of our reasoning. Uncertainty today is not just an occasional, temporary deviation from a reasonable predictability; it is a structural feature of the business environment. The method used to think about and plan for the future must be made appropriate to a changed environment".

He said this in 1985. I suggest readers peruse his September 1985 Harvard Business Review article entitled Scenarios: Uncharted Waters Ahead and several publications by Shell on scenario analysis (one of which is a book entitled Scenarios: An Explorer's Guide, written for people who would like to build and use scenarios).

Mental Model 3: Library of Mistakes

A few months ago, I visited an interesting liberal arts campus (Flame University) in Pune, India to learn about value investing and behavioural finance. They have an interesting collection of books that they named the 'Library of Mistakes'. This is the branch of the original library based in Edinburgh, Scotland.

The Library of Mistakes collects books and publications on financial and economic history. They gather materials on manias, panics, follies, euphoria and mistakes. The objective is to learn from mistakes and improve our understanding of how people, markets and economies work.

Munger advised everyone to "review your past stupidities so you are less likely to repeat them". Inspired by this idea (top it up with a little dash of inversion thinking), I started to collect and digest lessons from past mistakes and corporate failures as extensively as I could in order to learn what to avoid. As Munger said: "All I need to know is where I am going to die so I'll never go there". Studying mistakes help improve our cognitive skills and our ability to recognise patterns or hidden patterns from these mistakes.

Corporate Failures in 2018

This year, 2018, has been a volatile year. The year started with many people extrapolating perpetual optimism. Then, concerns on shifts in US monetary policy; escalation of the US–China trade war; emerging market debt problems for Turkey, Indonesia and Argentina; volatility in technology stocks; some concerns on the market cycle and many other seemingly random concerns.

These noises somehow brushed off several important corporate failures and mistakes that happened in 2018, including lessons we could learn from.

The fall from grace of Noble Group (which defaulted for the first time this year) provides some lessons on which early warning signals could provide clues on business and funding difficulties (read reports by research firm Iceberg Research enumerating the accounting anomalies done by Noble Group to hide debt).

The shutting down of Theranos – a health technology corporation – run by a once visionary start-up founder Elizabeth Holmes (who was compared to Steve Jobs). Read the book Bad Blood: Secrets and Lies in a Silicon Valley Startup written by John Carreyrou, which just recently won the Financial Times and McKinsey & Company Business Book of the Year Award 2018 and provides some insight into how envy makes extremely smart people do stupid things.

Companies in Turkey and other emerging market economies who borrowed in foreign currency and seemingly overlooked hedging these foreign-denominated debt, thinking that US rates would continue to be low forever, were caught off guard when their local currencies started to weaken and affected debt servicing. This again reminds us that you can fool some people all of the time.

IL&FS Financial Services Ltd. – owned by some of the state-owned companies in India and was initially promoted by the Central Bank of India, HDFC and Unit Trust of India – defaulted for the first time in 2018 due to liquidity problems.

Samsonite, a brand loved by many business travellers such as myself, encountered a small crisis as questions were raised on aggressive accounting practices, the CEO's résumé padding and manual journal entries that were allegedly revenue recognition management schemes.

The fall from grace of the once indispensable CEO/Chairman of Nissan and Renault, Davos Man and corporate superhero in Japan, Carlos Ghosn, is shocking to many, especially to myself who used to read books written by and about this dynamic CEO.

There are many other mistakes that we can cite. One good resource that the reader may want to read, especially relevant for banks with multiple risk dimensions (concentration, market, liquidity and credit), is the J.P. Morgan London Whale crisis (read the internal report published on the website of J.P. Morgan and official report by the US permanent subcommittee).

Learning From Short Sellers

Late this year, I attended a live online seminar, Advanced Seminar on Short Selling, conducted by famous hedge fund manager/value investor Whitney Tilson. I am not a short seller nor do I see myself engaging in this very asymmetric one-sided activity. Whitney, however, convinced me to attend this course to understand the mental, investment and risk management process of short selling.

Short sellers are rarely associated with risk managers. However, the mental process of short selling is something that risk managers would find valuable and applies the process of mental inversion quite well.

The mental discipline successful short sellers look for: Weak or dishonest management, low or negative growth, margins and return on capital, high and increasing debt, accounts receivable and inventory and weak competitive advantage. Whitney generously provided dozens of case studies on successes and failures throughout his 15 years of short selling.

Whitney admitted that short selling killed him. Risk managers can develop this sceptic mindset and learn to find hidden risks. I encourage everyone to enrol in this course and pick up some unconventional wisdom on risk management.

Conclusion

Munger has lived a long life with a successful track record of avoiding dangerous blind spots that allowed him to finish like a tortoise – slow and steady. He turns 95 in the coming year.

He is famously known as the 'abominable no-man' for his unconventional ways of thinking about investments. While Munger is growing in popularity, he is still relatively unknown as compared to Buffett.

He has raised some valid arguments against traditional finance and risk management models (for example, the use of volatility as a measure of risk, the capital asset pricing model and efficient market hypothesis). Einstein spoke about repeating the same mistake over and over again as the closest definition of insanity.

One clear conclusion from the 2008 financial crisis is that traditional risk management models have failed us. Perhaps, it is time to look for unconventional sources of wisdom and mental models to understand risks better.

Philip Te is the Vice President of Financial Markets structuring in a global commercial bank based in Singapore. He used to be with the Financial Services Risk Management group of Ernst and Young. He lectures extensively on risk management, hedging, derivatives and Basel II/III. He is a certified Financial Risk Manager, Energy Risk Professional, Chartered Financial Analyst and a Certified Public Accountant.

# FINANCIAL CRIME RISK MANAGEMENT IN ASIA PACIFIC

## A RISING COST & URGENT IMPERATIVE

How firms can get a **grip and prioritise.**

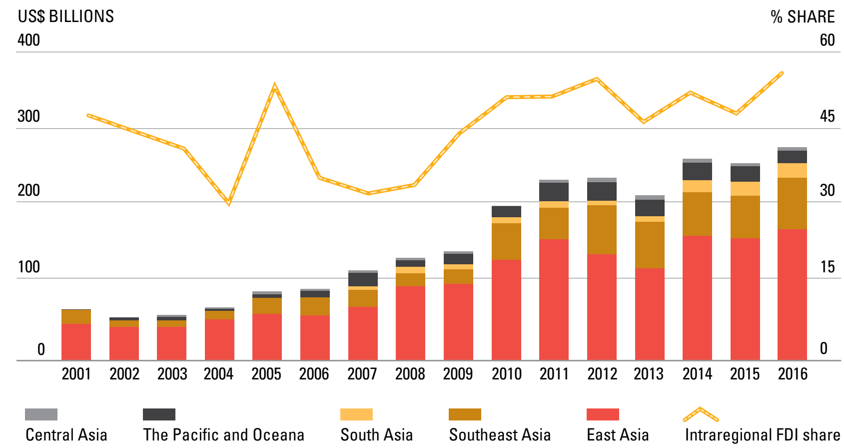
Costs for financial crime are rising and financial institutions in Asia are having to bear them. In February 2018, a large state-owned Indian bank was involved in fraudulent transactions of total value exceeding US$2 billion. As a direct cause of the market's reaction to the news, the bank's shares dropped by almost 40% of its market value in three weeks.

This happened due to the lack of adequate controls in the bank, which allowed criminals to work through the loopholes of the system and bribe internal employees to help them implement the fraud. While this has been dubbed as the biggest fraud in India's banking history, it is by no means an isolated incident in the region. This is an issue that financial services institutions all over Asia Pacific should deal with urgently, or the costs may become unwieldy for the industry and society at large.

### BANKS HAVE FAILED TO RECOGNISE THE LEGITIMACY OF MONEY

Asia has long been a key market of interest with consistent financial flows from the West. Foreign direct investment (FDI) is generally desirable for growing economies, not only in terms of immediate available cash flow for the local economy, but also in terms of

**EXHIBIT 1** **INTRAREGIONAL FDI INFLOWS—ASIA**




**SOURCE** Asian Economic Integration Report 2017, ADB

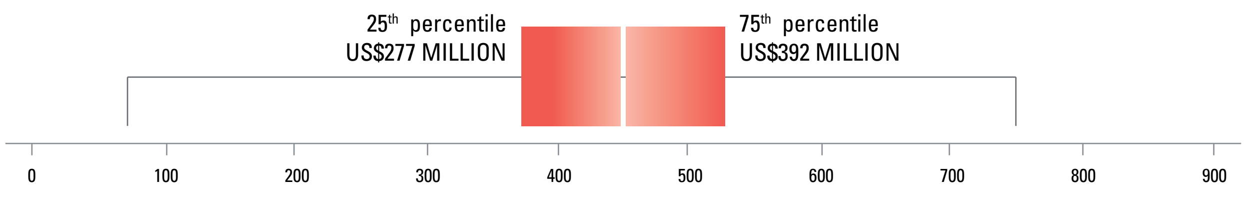
impact on local employment indices and socio-economic progress due to inundation of new ideas. However, countries often relax trade laws, foreign ownership rules and government processes in order to make their country business- or investment-"friendly". This may affect the country's ability to effectively assess and manage the legitimacy of incoming cash flows. Recent trends in Asia indicate that intraregional FDI has been on the rise in the region (see **Exhibit 1**).

With over 50% of FDI in Asia coming from other Asian countries, the overall development in the region is strongly dependent on the financial health and stability of the Asian market as a whole. This underscores the need to ensure that incoming capital is robust and reliable.

Yet, the incoming cash flows are by no means all legitimate. Apart from carrying cash into a country, banks serve as the only "on and off ramp" for the payments system, and are the nexus through which all foreign money flows. However, banks have had a history of spectacular failures in risk management, most notably the failure to identify payments and transfers that cause a breach in sanctions, and accusations of being complicit in money laundering schemes. The latter issue has specifically plagued a multinational British bank, which was accused of being complicit in sovereign money laundering of a staggering GBP191.8 billion (approximately US$254.7 billion) over 10 years. Perhaps the magnitude of the amount involved is best fathomed in relative terms – a single transaction of this order would likely wipe out quarterly profit for all but the


**+ However, banks have had a history of spectacular failures in risk management, most notably the failure to identify payments and transfers that cause a breach in sanctions, and accusations of being complicit in money laundering schemes.**

**EXHIBIT 2 LARGE SCALE FINANCIAL CRIME CONTROL TRANSFORMATION PROGRAMS, TYPICAL SPEND (US$ MILLION; EXCLUDING REMEDIATION COST, TOTAL SPEND OVER 3-5 YEARS)**




largest 50 banks in the world.

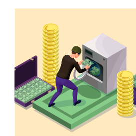
Considering the extensive inflow of foreign funds, it is especially imperative for Asian banks to actively manage and mitigate risks associated with financial crime. This will not only help limit freedom of criminals and rogue states to operate, but also serve as a simple protection against financial distress and build trust in society.

## A FOCUS FOR GOVERNMENT

Nearly all developing economies have substantial trade in the "black" market. This is a broad term used to refer to the untaxed, cash and foremost illegal transactions, which is frequently associated with serious crime, occasionally including terrorism funding. All the associated financial flows ultimately touch the banking sector, and governments all over the region have been steadily ramping up its resources and regulations in order to crack down on financial crime and its actors:

+ The Monetary Authority of Singapore (MAS) is known for its zero-tolerance approach to financial crime and has historically taken strict action against any breaches or violations. From 2016 to 2017, the Singaporean branches of two Swiss-based banks were shut down and senior executives prosecuted for failing to control money laundering activities connected with an Asian sovereign wealth fund. Other local and foreign banks that were considered in violation of Singapore's anti-money laundering laws were slapped with sizeable fines of over SGD1 million each. Following this major breach, the MAS set up dedicated units to monitor money laundering risks and boost enforcement action.
+ The Hong Kong Monetary Authority (HKMA) also launched a Fraud and Money Laundering Intelligence Taskforce in May 2017. The taskforce was launched as a 12-month pilot and is a collaborative effort between the HKMA, Hong Kong Association of Banks, and 10 retail banks with a single aim of enhancing detection, prevention and disruption mechanisms to combat financial crime.
+ An extreme case of government action was documented in Vietnam in December 2017, where the former board chairman of a large privately owned bank was handed a life sentence over charges of embezzlement and money laundering.

Other governments have directly enhanced funding to programmes that track suspicious activity:



**+ Considering the extensive inflow of foreign funds, it is especially imperative for Asian banks to actively manage and mitigate risks associated with financial crime.**

The annual budget of the Australian Transaction Reports and Analysis Centre (AUSTRAC) has been increasing in line with the increased proliferation in financial crime. In 2010, AUSTRAC's annual budget was AUD79.9 million. The estimated actual budget for 2016–17 was upped to AUD88.6 million by the government with additional funds made available for recruiting appropriately skilled staff.

In December 2017, the Australian Minister for Justice Michael Keenan announced a new funding package to inject an **extra AUD43.3 million** (~50% of the announced budget) "to allow AUSTRAC to recruit more staff to ensure our financial institutions comply with the AML/CTF law and AML/CTF Rules". This injection is a significant statement of intent by the Australian government and AUSTRAC to reporting entities to ensure they have in place appropriate responses to their AML/CTF obligations.

## THE IMPERATIVE FOR REGULATED FINANCIAL INSTITUTIONS

Regulators in the Asia-Pacific region will expect much more of the banks in terms of monitoring, controls and reporting, and banks will have to move closer to international norms in terms of investment in preventing financial crime. In terms of cost, we expect most banks to at least double their annual spend on financial crime risk management in business-as-usual state. Additionally, many banks that are coming from a lower base will need to significantly upscale their financial crime control environment to meet international norms.

Estimates for large-scale financial crime control transformation programmes range from US$52 million to over US$111 million annually (average spending by industry leaders and large banks, excluding remediation cost) of which 10–20% will continue to accrue annually in business-as-usual state (see **Exhibit 2**).

At the lower end of the spectrum are typically domestic banks with a limited international footprint. Such banks are characterised by:

- less stringent local regulations and/or low regulatory intervention;
- institutions with historically higher levels of investment in financial crime control; and
- greater use of internal resources, only leveraging external advisors in key SME roles.

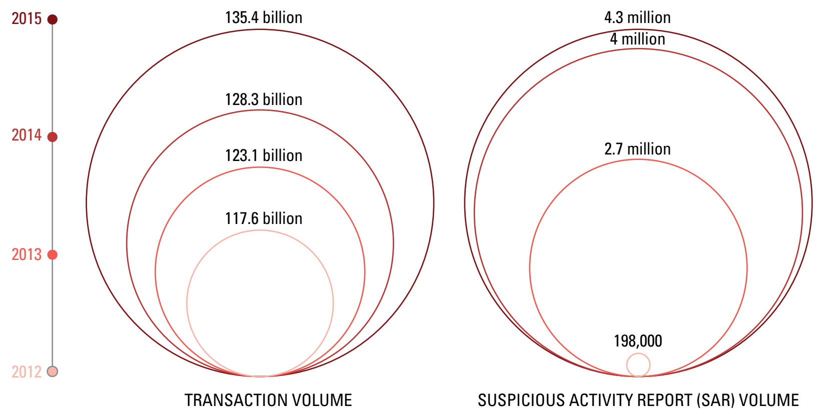
At the higher end of the spectrum are large global universal banks with the following characteristics:

- significant regulatory intervention/ findings;
- historical underinvestment in financial crime control programmes;
- higher global minimum standards, e.g. global application of US standards; and
- high dependency on external advisors, e.g. advisory, legal and specialist SMEs.

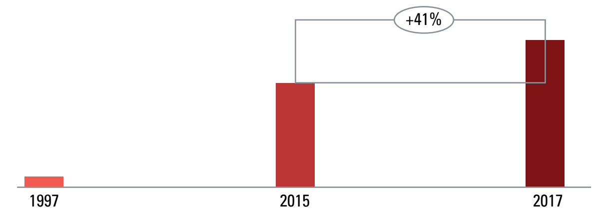
Asian banks should align themselves to where they want to be in future, instead of where they map at present. Banks can take a cue from peer jurisdictions here:

- The US saw a shocking 20x increase in Suspicious Activity Report (SAR) filings in just 3 years (between 2012 and 2015) while growth in transactions increased moderately by approximately 3% between 2013 and 2015 (see **Exhibit 3**).
- Closer to home, a similar increase

**EXHIBIT 3 RECENT TRENDS IN TRANSACTION VOLUMES AND SUSPICIOUS ACTIVITY REPORT FILINGS IN THE USA***




Number of suspicious activity reports files with JFIU in Hong Kong




***SOURCE** BIS Committee on Payments and Market Infrastructure. Statistics on payment, clearing and settlement systems in the CPMI countries. Figures for 2015. December 2016; FinCEN SAR Stats. Technical Bulletin. March 2017; Data includes reports for money laundering, fraud, mortgage fraud, casinos, identification documentation, insurance, secruities/futures/options, structuring, terrorist financing, and other suspicious activities.

**SOURCE** *South China Morning Post,* Wednesday, 2 November 2017

## SIX THINGS TO DO NOW

**1 COMMUNICATION**
- Top-down communication on importance of controls
- Active involvement from senior ocials in educating the organisation

**2 CULTURE**
- Risk awareness should be embedded in the culture of the bank
- Bankers are expected to be well-versed with details of each transaction

**3 COMPLIANCE**
- Compliance and reporting should be at expected levels
- Staff at all levels should be aware of relevant requirements

**4 COVERAGE**
- All customer segments, product classes, geographies, etc. should be included for monitoring

**5 COMPUTATION**
- Banks should effectively leverage analytics and robotic process automation to monitor transactions and identify likely criminal activity
- Results in highest gains without excessive manpower deployment

**6 COOPERATION**
- Cooperation between banks on "best practices" in risk management
- Sharing critical information such as KYC utilities

in reporting of suspicious activities is noted by the Joint Financial Intelligence Unit (JFIU) in Hong Kong. The JFIU received more SARs from banks in 2017 than in any single year since their inception in 1989. This increase has been linked with the HKMA's requirement for banks to focus resources on the identification, assessment and filing of SARs.

While SAR filings have also been increasing in other major financial centres around the world with annual growth rates of 11% between 2012 and 2016, those rates have been far lower than the ones experienced in the US or Hong Kong markets, while increases in transaction volumes have been similar across the major financial centres such as US, Singapore, Hong Kong or Australia.

**+ The differences observed in SAR filings growth rates can generally be attributed to three factors:**

1. Either there is indeed more suspicious activity in the US and Hong Kong markets compared to other financial centres; or

2. Regulators in other jurisdictions are less stringent on reporting activities; or

3. US and Hong Kong regulators are much more sensitive with what constitutes suspicious activity and the reporting requirements it imposes on the entities operating within their jurisdiction.

In any case, the numbers show that even in sophisticated markets, financial crime operations are not yet fully effective – especially given that regulators have observed that only 10–20% of reported SAR filings actually add value to active law enforcement investigations.

We therefore expect that regulators in many affected markets will keep raising demands on their reporting entities and that the pressure and need to raise awareness and investment will not go away. In order to remain relevant to their international competitors, Asian banks need to invest heavily in non-financial risk management in general, and specifically, to manage financial crime. Inaction may result in extensive regulatory and supervisory implications in the future, including fines, stricter capital, compliance rules and severe reputational damage, and loss of trust with customers.

### SIX THINGS TO DO NOW

Many firms that find themselves early in the journey of investing in financial crime risk management may struggle to know where to start and how to get a grip on the issues and their priorities.

The first step is getting a handle on the issues and establishing a good relationship with the regulator. Most supervising bodies appreciate the complexities with which the bank is dealing. They are aware that controls sometimes represent a trade-off with customer experience, that systems may themselves prevent the creation of perfect controls environments, and that cultures and behaviours are slow to change.

Nevertheless, their expectations have moved and we suggest an action plan targeting six areas for gains to get started:

❶ **Communication.** Senior leadership need to cascade communication of the importance of financial crime controls. Cultural gaps will begin with expectations from leadership; the Board and Executive Committees need to be well versed in specific examples of failures of financial crime controls and their implications. These can then be used to educate their leadership teams in the importance of world-class risk management in this area.

❷ **Culture.** Uncertainty about the purpose of a transaction and identity of a customer must be unacceptable in the culture of the organisation. This will be critical not just for management of financial crime, but also for good conduct and to satisfy community expectations. The playing field of expertise in finance is not level between provider and customer; bankers will be expected to have a solid grasp of transaction logic. Unusual requests should be met with questions, not executed regardless. This can be turned into a competitive advantage if done well and seamlessly.

❸ **Compliance.** All staff need to understand the organisation's obligations for clear and transparent reporting to regulatory and supervisory bodies. Staff should be aware of their role within that overall obligation. Compliance must be a 'gate' for performance measurement and a basic requirement at all levels.

❹ **Coverage.** Technical aspects of managing financial crime are equally important – all transactions need to be screened, and all customers need to go through Know Your Customer (KYC) procedures to the desired quality. Risk assessments need to be thorough and scenarios tested need to be comprehensive to cover all products and segments. All geographies, branches, and subsidiaries need to meet minimum standards, which are well articulated and understood.

❺ **Computation.** While financial crime is a major issue for all banks, armies of people conducting transaction checks and monitoring is not the answer. The most advanced institutions are finding radical increases in productivity from analytics. To this end, Citigroup president and chief executive of the bank's institutional clients group, Jamie Forese, believes that the bank could replace up to half of its 20,000 technology and operations staff with machines over the next five years. According to Mr Forese, operational positions at the bank were "most fertile for machine processing". It is an increasingly common sentiment. Transaction monitoring is moving from merely screening to use of advanced analytics and machine learning. This, by prioritising the files for manual review, skews focus of expensive expert time to cases where it is most needed. Large complex organisations such as HSBC have realised double digit gains in productivity and helped set the goalpost for the industry.

**The cost of poor financial crime risk management falls heavily on society as a whole – but especially heavy on the pockets of shareholders in firms judged to have materially missed expected standards.**

❻ **Cooperation.** There are areas where cooperation in the industry is possible and to everyone's benefit, such as in the creation of utilities for processes that meet KYC requirements. Well-targeted cooperation makes regulators more, rather than less, comfortable; customers more satisfied (assuming privacy can be handled appropriately); and banks more efficient (where incentives are aligned).

The cost of poor financial crime risk management falls heavily on society as a whole – but especially heavy on the pockets of shareholders in firms judged to have materially missed expected standards. The response needs to be broad and deep, raising seniority of issue ownership, capabilities, and engagement at all levels of industry. Leaders have already made substantive moves. Where is your firm? ✱

■ *Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.*

# Trust in the Digital Age

## BUILDING A CYBER RESILIENT FINANCIAL INSTITUTION

Highlights from the latest joint study assessing financial institutions' **cyber risk maturity and resilience.**

**+ Cyberattacks are now so numerous and sophisticated that some attacks will inevitably get through even with the most robust defence capabilities.**

Trust has always been a core value for banks in delivering their services, a big part of which includes ensuring the safety and security of customer assets. But the security of financial institutions has now come under immense threat, judging from the many high profile news reports of reputable and trusted multinational and local banks falling prey to cybercrime attacks, both internally and externally.

## YET ANOTHER CYBER INCIDENT MAKING HEADLINES

At the time of writing, another major breach was reported. Attackers had gained access to the UK-based HSBC Bank's customer information in the US. It is believed that they stole sensitive personal data from Internet banking services, including account balances and statement histories.

Clearly, traditional cybersecurity strategies, such as firewalls and intrusion detection systems, alone are no longer enough to prevent determined threat actors. Cyberattacks are now so numerous and sophisticated that some attacks will inevitably get through even with the most robust defence capabilities. Cybersecurity should therefore be about the management rather than elimination of cyber risks. This means security needs to go beyond systems, software or IT departments and establish procedures and protocols for governance oversight, culture, risk identification, protection, detection, response and recovery.

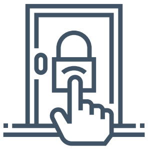
## THE REVISED BNM GUIDELINES ON TECHNOLOGY AND CYBER RISK MANAGEMENT

In September, Bank Negara Malaysia (BNM) published the exposure draft, *Risk Management in Technology (RMiT) Guidelines.* The Guidelines set out BNM's expectations of financial institutions' technology and cyber risk management. It lays out standards and guidelines proportionate to the size and complexity of the financial institutions. BNM is currently seeking for written feedback on the proposals in this exposure draft, including suggestions on areas to be clarified and alternative proposals that they should consider.

According to the exposure draft, at least nine other guidelines and circulars issued to financial institutions in the last decade in relation to securing, safeguarding and protecting the information infrastructure and system implemented by financial institutions will also be replaced.

The *RMiT Guidelines,* once finalised, will supersede *BNM's Guidelines on Management of IT Environment* issued in May 2004. According to the exposure draft, at least nine other guidelines and circulars issued to financial institutions in the last decade in relation to securing, safeguarding and protecting the information infrastructure and system implemented by financial institutions will also be replaced.

Amongst many things, here are some of the key highlights from the *RMiT Guidelines:*



### INCREASED INVOLVEMENT BY THE BOARD AND SENIOR MANAGEMENT IN MANAGING CYBER RISK

- Boards and Senior Management will be responsible for establishing the Technology and Cyber Risk Management framework. It also requires the Board to allocate sufficient time to discuss cyber risks, and have at least one Board Member with technology experience and competencies in order to facilitate a more effective discussion.

### NEED FOR A DEDICATED FUNCTION OUTSIDE OF IT TO MANAGE CYBER RISK

- Senior Management must establish a dedicated oversight committee to provide strategic and operational guidance on technology. Members of the oversight committee must include Senior Management, not just from technology functions but also the major business units.
- Financial institutions are also required to establish an independent enterprise-wide technology risk management function led by an executive member, i.e. Chief Information Security Officer who shall be independent from current day-to-day technology functions.

### INTELLIGENCE-LED SECURITY ASSESSMENT OR "RED TEAM" EXERCISE

- Ability to understand the current threats the organisation is exposed to and conduct intelligence-led penetration testing on its internal and external network infrastructure as well as the critical application system, including web, mobile and all external facing applications.

- Proactively test and simulate sophisticated "Red Team" attacks on its current security controls and identify potential vulnerabilities, including infrastructure hosted with third-party service providers.

### ESTABLISHING A "BLUE TEAM" TO PERFORM THREAT HUNTING

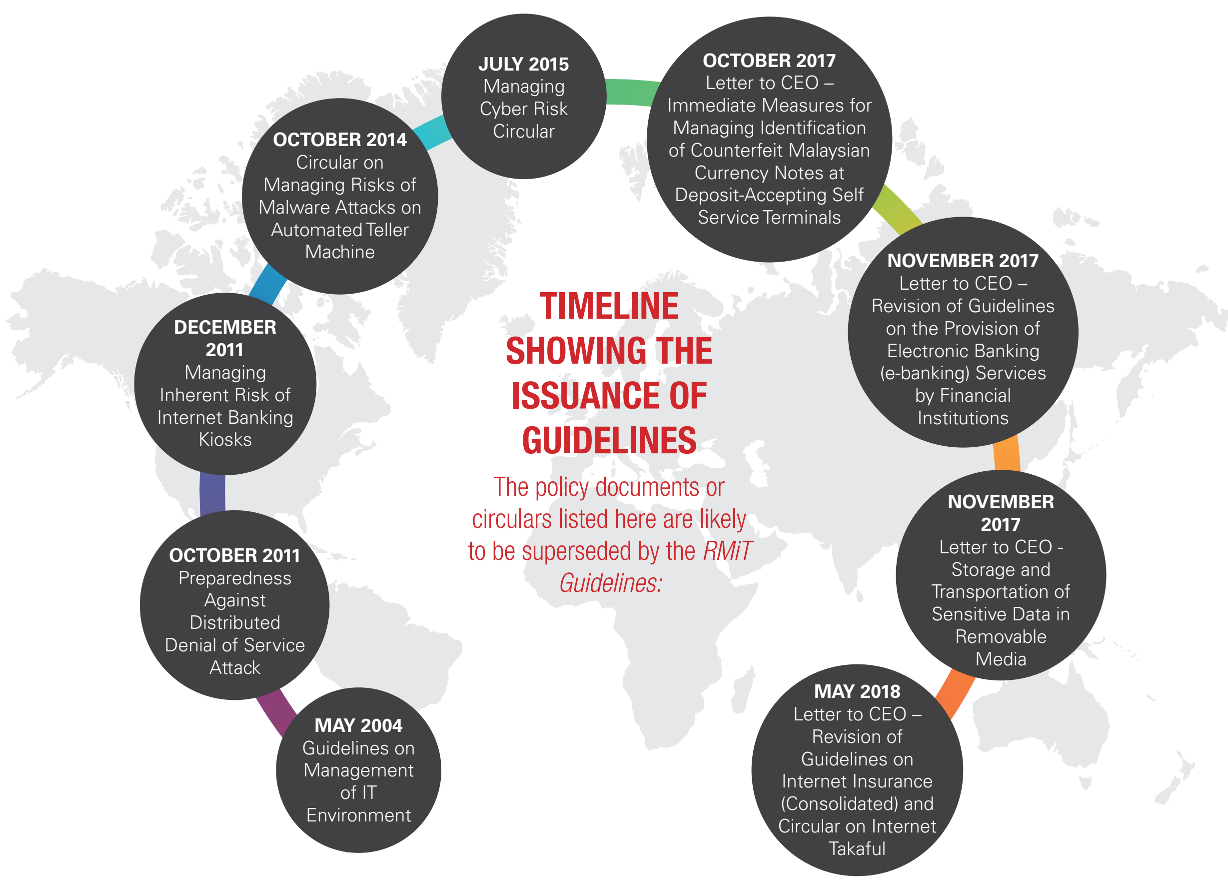
- Large financial institutions are now required to establish an internal security function, or "Blue Team", within the financial institution's technology department to continuously detect, defend and prevent potential compromise of its security controls or weakening of its security posture. This includes performing quarterly vulnerability assessment of external and internal network components that support all critical systems.

### EFFECTIVE CYBER HYGIENE PRACTICES

- Recognising that most cyber breaches occur due to poor cyber hygiene, BNM has provided more prescriptive guidelines and standards on security standards expected of financial institutions, i.e. multi-factor authentication, cryptographic controls and key management, security patch management, etc.

### A PLAYBOOK TO RESPOND TO CYBERATTACKS

- Financial institutions must establish a comprehensive Cyber Incident Response Plan (CIRP). Each organisation needs to conduct an annual cyber drill exercise to test the effectiveness of CIRP based on various current and emerging threat scenarios (e.g. social engineering) with the involvement of key stakeholders, including members of Senior Management, the Board and third-party service providers.



In the last 12 months, we have seen regulators and central banks of many developed markets continue to revisit the existing cybersecurity guidelines to keep pace with the velocity of technological changes and the threat landscape. In the EU for example, the European Central Bank has published the TIBER-EU Framework to guide financial institutions on how to implement the European Framework for Threat Intelligence-based Ethical Red Teaming.

Closer to us, the Monetary Authority of Singapore has issued a *Notice on Cyber Hygiene* prescribing a set of essential cybersecurity practices that financial institutions need to put in place to manage cyber threats. Our local financial institutions with presence in these countries are already taking steps to comply with these new requirements. The *RMiT Guidelines,* if implemented, will help elevate the security standards and practices of local financial institutions and be on par with the more developed markets, to protect and defend themselves against cyber adversaries. This is indeed a significant and positive step forward. The question now is: How ready are local financial institutions for the new regulatory and supervisory guidelines?

## WHAT WE FOUND FROM OUR SURVEY

Between July and August this year, the AICB and PwC Malaysia conducted a study on local financial institutions to gauge their level of maturity in managing cyber risk and staying resilient in the event of a cyberattack. The survey drew responses from Board Members and executives from more than 10 local banks including foreign banks with local operations and local development finance institutions.

**Some of the key findings found from our survey include:**

### CYBER RISK GOVERNANCE NEEDS TO BE STRENGTHENED – CYBER RISK NEEDS TO BE SEEN AS A BUSINESS RISK, NOT AN IT RISK.

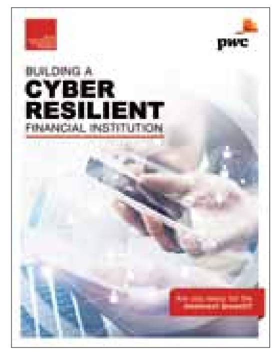
### THE PROBLEM: SECURITY, NOT RESILIENCE

While information security risks have dramatically evolved over the past few decades, the approach used by financial institutions to manage them has not kept pace. Cyber risks are still largely seen as an IT risk and not a business risk:


More than 70% of Malaysian banks still rely on their existing IT security or IT operations to perform cybersecurity-related functions and responsibilities.


58% of Board Members from Malaysian banks indicate that the reporting of cybersecurity matters is still predominantly performed by the CIO or CTO.

Between July and August this year, the AICB and PwC Malaysia conducted a study on local financial institutions to gauge their level of maturity in managing cyber risk and staying resilient in the event of a cyberattack.




Based on our survey, a majority (40%) of the banks surveyed agreed that the full Board has primary responsibility for overseeing cyber risks, and challenging management assumptions. However, 70% of the respondents indicated that current capabilities are not sufficient.

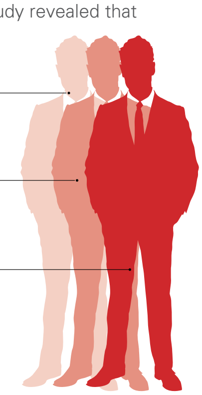
### BOARD-LEVEL CAPABILITIES

Boards are expected to assume greater responsibility for ensuring an organisation's cyber resilience. Our study revealed that directors recognise a clear need for more cybersecurity capabilities on their Boards.

**10%** say they have it

**20%** say they don't have it

**70%** believe they have some capabilities, but require more



### LACK OF A 'THREAT-LED' OR INTELLIGENCE-LED CYBER RISK MANAGEMENT PROGRAMME.

While banks are generally reaching out to keep themselves updated on cyber threats, they tend to rely on generic industry conferences and their vendors as sources of information as opposed to sources specific to them, i.e. from other financial institutions as well as their own threat intelligence.

When asked "Where do you normally obtain sources of updates and developments on cyberthreats?", our survey respondents replied:

## SOURCES OF UPDATES AND DEVELOPMENTS ON CYBERTHREATS

#1 Industry Conferences & Events

#2 Vendors & External Consultants

#3 Peers in the Industry

#4 Subscribed Threat Intelligence

#5 Regulators & Others

Our survey results demonstrate a clear need for banks to focus on building a threat-led cyber risk management programme:

48%

Only 48% of banks surveyed subscribed to threat intelligence and actively monitors / analyses it to detect risks and incidents.

Of that 48%, the majority (60%) come from IT while less than 40% come from Risk and Compliance. There is room for banks' second line of defence to greatly leverage threat intelligence to embed it into overall risk treatment strategies.

## LAGGING BEHIND WHEN DEALING WITH THIRD-PARTY RISKS.

Local banks are lagging behind when dealing with third-party risks

When asked how often banks perform a review of their service providers, the majority of respondents indicated that they do this on an annual basis.

3%

With only 3% of respondents adopting a risk-based approach when deciding on the frequency of the review.

Such practices are driven by lower third-party-related incidences for banks in Malaysia.

Only 21% of respondents quoted third parties as a source of security incidents in the last 12 months. Meanwhile, the survey also revealed that 34% of respondents do not know the root causes of their security incidences.

21%

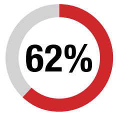
By contrast, incidents related to compromised third parties were recorded as one of the top security incidents by the financial services respondents in PwC's Global State of Information Security Survey (GSISS) 2018

48%

About half (48%) of the financial services respondents from GSISS 2018 indicated that their security incidents in the last 12 months were attributed to third parties, including service providers, contractors and vendors.

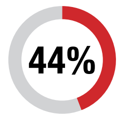
## ABSENCE OF A BLUE OR RED TEAM MAINLY ATTRIBUTED TO LACK OF STRONG SECURITY CAPABILITIES.

The majority of banks do not have a Blue or Red Team established within their current security team. The current monitoring capabilities practiced by banks are mostly in terms of monitoring of alerts and require new skill sets such as the ability to perform correlation of threat intelligence feeds with network logs and perform threat hunting.




62% of respondents ranked penetration testing and vulnerability assessment among the top 3 in terms of security spending.

44% of respondents indicated that they have not considered any "stress testing" using the Red Team exercise, or ranked such an exercise among the lowest 3 in terms of security spending.




### CYBER HYGIENE CONTINUES TO BE THE MAIN REASON FOR BREACHES/SECURITY INCIDENTS.

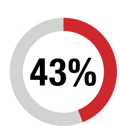
Respondents ranked cyber hygiene issues such as traditional software vulnerabilities No. 2 in the list of contributors for security incidences occurring in the last 12 months within their organisations.

### INDUSTRY SHARING AND COLLABORATION IS NOT SUFFICIENT, MAKING FIGHTING CYBERCRIME INEFFECTIVE.

Like how most Malaysian households form neighborhood associations to deal with domestic security issues, the concept of *Rukun Tetangga* can be applied to corporates in joining forces to fight cybercrime.


100% of respondents agreed that it is important to collaborate with others in the industry, including competitors, to improve security and reduce potential future risks.

43% However, only of respondents indicated that current sharing and collaboration methods practiced within their organisation are sufficient to manage cyber risks.




However, such collaborations are currently not in place, making it ineffective and inefficient for financial institutions to deal with their adversaries, who seem to form better alliances and have better shared intelligence, i.e. the dark webs of their prey.

---

It is apparent from our survey that there is still a lot work to be done to address the requirements and standards spelled out in the guidelines. The industry may continue to debate on its ability to comply with such guidelines in full. However, adopting an effective cyber risk management strategy is no longer a nice-to-have, but a necessity. After all, the intent of such regulatory and supervisory frameworks is to provide local financial institutions a baseline of standards that will challenge them to be more ambitious in pursuing cyber defences to stay resilient in the face of the imminent breach.

## WHAT NEEDS TO BE DONE

More emphasis on the following areas is required for banks to strengthen their organisations' resilience towards the imminent breach. This includes:

- Building a threat-led cyber risk management programme
- Cultivating a culture of sharing and collaboration
- Stress testing your cybersecurity defence
- Getting the basics right

### THE WAY FORWARD – NO TIME TO WASTE

A major takeaway from the survey is the notion that improved cyber risk resilience can lead to stronger economic performance. Financial institutions of all sizes across all sectors and locations need to look inward, evaluate their approach to managing cyber risk and start focusing on becoming more cyber resilient. The need to foster cyber risk culture and perceive cyber resilience as being a part of business operations has never been greater.

For those leading the charge to strengthen cyber resilience in their organisations, the task entails expanding their understanding of the business and sphere of influence and communicating clearly the existing and potential cyber risks in terms of business impact. For CEOs and Board Members, particularly, it means being fully engaged in the process, asking the tough questions and taking a closer look at the organisation's cyber risk management strategy and risk mitigation programme. ✱

■ *Authored by Tan Cheng Yeong, Partner, PwC Malaysia Digital Trust & Security Leader; and Clarence Chan, Associate Director, PwC Malaysia Digital Trust & Security.*

***Building a Cyber Resilient Financial Institution: Are You Ready for The Imminent Breach?*** *is a thought leadership and survey publication developed by AICB in collaboration with PwC. AICB continuously promotes thought leadership through various platforms and collaborative initiatives to ensure members are kept abreast of current issues affecting the banking industry. This publication aims to provide greater insight and awareness on the state-of-play in the domestic and global landscape of cybersecurity, with a strong focus on the shift towards cyber resilience and what it means for businesses as they reshape their strategies to be fit and ready for the future.*

 | BY JULIA CHONG

# THIRD-PARTY RISK: GETTING TO LOCKDOWN

You can outsource the work, but you **can't outsource the risk.**

Even the best-laid plans can unravel when it involves external or third-party vendors at any point of the value chain.

As financial institutions (FIs) turn to outsourcing of work functions like customer service, audit, security, facilities management, IT, document management, and form new synergistic partnerships with fintech for efficiency gains, the scope of risk is increasingly multifold and multidimensional.

Third-party vendors may prove to be one of the weakest links. Time and again, cybercriminals have exploited this vulnerability to, quite literally, break the bank.

2016's Bangladesh Bank cyber heist (see p.XX) is proof positive that banks cannot assume zero failure of their systems at any point in time, and protocols for lockdown must be clearly defined from onset.

DIAGRAM 1

## 10 STEPS TO IMPLEMENTING AN EFFECTIVE THIRD-PARTY RISK MANAGEMENT PROGRAMME

### STEP 1 ▸ ESTABLISH ROLES & RESPONSIBILITIES

Begin implementation by establishing a third-party risk management policy that makes clear where the programme's authority resides and clearly defines roles and responsibilities. Banks and financial services companies with a more mature model centralise third-party risk within their enterprise risk management or operational risk management functions. Centralising the third-party risk management programme in

this way provides the authority to support cross-functional collaboration among the procurement, contracting, and legal departments. In addition to representatives of these functions, the implementation team should determine risk domain subject matter experts in the areas of information security, compliance, physical security, privacy, finance, business resiliency, and any other areas where there may be significant inherent risk for the firm.

### STEP 2 ▸ INVENTORY THIRD-PARTY RELATIONSHIPS

Identify and inventory traditional and non-traditional third-party relationships throughout the organisation and map third-party relationships to the company's business processes, products, or services. The best place to begin identifying and

inventorying third-party relationships is in accounts payable, since many of these relationships will eventually generate payments.

Similarly, examining receivables can reveal non-customer revenue sources

A bank's use of third parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws.

## CULTURE OF VIGILANCE

To rein in third-party risk, banking rule-makers prescribe that FIs instil a culture of vigilance by defining the boundaries of responsibility for all stakeholders.

This approach to third-party risk management programmes (TPRM) – also known as third-party oversight or vendor management – has spawned the ubiquitous term "you can outsource the work, but you can't outsource the risk", with ultimate responsibility falling squarely on the shoulders of directors and executive management.

Unlike other aspects of banking, there is no universal standard when it comes to managing third-party relationships. The closest there is to a comprehensive common framework in a jurisdiction is the US Department of the Treasury's Office of the Comptroller of the Currency (OCC) Bulletin 2013-29, *Third-Party Relationships: Risk Management Guidance,* issued 30 October 2013, which outlines:

"The OCC expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party.

"A bank's use of third parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws.

"Many third-party relationships are subject to the same risk management, security, privacy, and other consumer protection policies that would be expected if a national bank were conducting the activities directly."

## SUBSEQUENT PARTIES

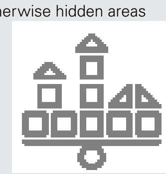
Getting to deep third-party transparency is arduous. Today's TPRM programmes extend to fourth- and fifth-parties, include due diligence procedures, and oversight of subcontractors for the renewal or termination of contracts.

In Asia Pacific, FIs involved in the cross-border transfer of information in Europe and the US must adhere to the data protection regimes in these jurisdictions and also ensure adequate and ongoing mechanisms are in place

that should be inventoried. The implementation team could also examine the company's referral agreements and catalogue the parties that have access to its information systems and physical facilities.

In addition to traditional suppliers of goods and services, the inventory should include: joint marketing agreements | settlements, e.g. debt collectors | affiliates, joint ventures, and intragroup arrangements | fourth parties, e.g. third-parties' subcontractors.

Each relationship should be mapped to business processes and the company's products and services to identify areas of potential risk concentration. This is also helpful for identifying otherwise hidden areas



where regulatory compliance risk may be high. Finally, the third-party risk management programme should establish control processes to assess the completeness of the inventory.

### STEP 3 ▸ ASSESS INHERENT THIRD-PARTY RISK

With a complete inventory in hand, the next step is to assess the inherent risks related to the various relationships. The team should base these assessments on its understanding of the nature of the products and services offered by the third party and the impact they may have on the bank or financial services company. Assessment criteria should include: in and out of scope | criticality | access | geography | resiliency and viability.

### STEP 4 ▸ PERFORM ENHANCED DUE DILIGENCE (EDD)

For relationships that warrant further assessment, perform EDD, including control assessments, and identify, document, and communicate unmitigated control weaknesses or gaps. This process often involves subject matter experts.

It's important to consider how well the company or third party is controlling inherent risks. Perform a gap analysis to determine current and future goal states. Discuss remediation plans with the third party and establish exception

## Banks Fall Prey to Cyber Heists Via Swift Platform

Sometime between 4 and 5 February 2016, Bangladesh Bank fell victim to an anonymous hack with a reported US$81 million stolen in one of the world's biggest attacks yet through a third-party system.

Forensics indicate that criminal hackers had manipulated SWIFT's Alliance Access software, using SWIFT credentials of employees of the Bangladesh central bank to send over three dozen fraudulent money transfer requests. The requests for the total US$1 billion transfer was received by the Federal Reserve Bank of New York for Bangladesh Bank's funds to be channelled to accounts in Sri Lanka and the Philippines. The transfer was in process when a typo made by hackers alerted bank officials who halted its completion.

Some amounts have been recovered from casino junkets in Manila but much of it remains lost. It was later discovered that Dridex, a malware that specialises in stealing bank credentials via a system that utilises macros from Microsoft Word, was deployed in this attack.

This heist inspired a copycat US$2 million cyberattack at India's City Union Bank on 6 February 2018. The hackers' tactic – deployment of a malware to disable the printer connected to SWIFT – occurred despite City Union's upgraded security features, which took place a day before.

Its CEO said in a phone interview with *Reuters:* "Nobody suspected that it was an attack and thought it was a systemic network failure."

After City Union's attack, the Central Bank of the Russian Federation also admitted that unidentified hackers had spirited away RUB339.5 million (approximately US$6 million) from a Russian bank last year – also via SWIFT.

whenever there is onward transfer of personal data, reflected in new laws such as the Australian Privacy Principles and Hong Kong's Personal Data Privacy Amendments.

By now, all FIs should, at the very least, have in place a baseline TPRM programme. The market has invariably matured and deeper insights have led to its next stage, dubbed 'effective TPRM' by industry, with emphasis on the opportunity to create business value whilst fulfilling regulatory obligations.

Advisory firms like Crowe LLP have issued guidelines that assist banks in their transformation towards effective TPRM (see Diagram 1), capturing the broad base of what's expected in an operational strategy.

### BROAD BY DESIGN

Many early adopters bore the initial brunt of frustrations, underestimating how deeply complex TPRM is intertwined with every service level and business line.

In response to this, subsequent guidelines such as the OCC's *Frequently Asked Questions Supplement* to Bulletin 2013-29 on 7 June 2017 clarified some common concerns, summarised below:

> **Not all risks are equal:** Third-party relationships present varying levels of risk across banks. Subsequently, banks should adjust risk management practices – due diligence, ongoing monitoring, appropriate documentation – to be commensurate with the level of risk and with periodic updates throughout the relationship.

> **No single structure:** Some banks have

DIAGRAM 1

### 10 STEPS TO IMPLEMENTING AN EFFECTIVE THIRD-PARTY RISK MANAGEMENT PROGRAMME

tracking and approval processes to monitor progress and assess performance.

**STEP 5 DEVELOP & TRACK ACTION PLANS**

The due diligence process can result in findings that require resolution. For each finding, establish an action plan internally and with the third party to mitigate identified control weaknesses or gaps, and make sure to track them through completion.

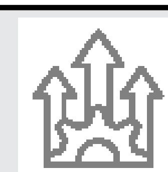
**STEP 6 CREATE ASSESSMENT-DRIVEN CONTRACT CLAUSES**

Finalise a contract for the relationship and include assessment-driven clauses and components such as: a requirement to participate in

risk management activities | the right to audit relevant processes | service level agreements | policy and approval processes for subcontractors (fourth parties) | notification requirements covering significant changes and adverse events | regular meetings and reports.

**STEP 7 FORMULATE ONGOING MANAGEMENT ACTIVITIES**

Ongoing management activities include regular or continuous monitoring for contract compliance, adverse events, and change, which



can be streamlined using technology. It should also establish processes for internal monitoring of change, such as new or modified statements of work, changes in data provided, and changes in access to networks and physical

By now, all FIs should, at the very least, have in place a baseline TPRM programme. The market has invariably matured and deeper insights have led to its next stage, dubbed 'effective TPRM' by industry, with emphasis on the opportunity to create business value whilst fulfilling regulatory obligations.


dispersed accountability, others have centralised the process. Irrespective of structure, the board is responsible for overseeing the development of an effective TPRM process. Periodic board reporting is essential to ensure that board responsibilities are fulfilled.

> **Collaboration is useful but insufficient:** Using the same service providers to secure or obtain like products or services, banks may collaborate to meet certain expectations, such as performing due diligence, contract negotiation, and ongoing monitoring, but products and services may, however, present a different level of risk to each. Collaboration can distribute costs across multiple banks but it may not fully meet due diligence, contract negotiation, or ongoing responsibilities. Banks may engage with a number of information-sharing organisations to better understand cyberthreats to their own institutions as well as to the third parties with whom they have relationships.

> **Is fintech a critical activity?** Addressing recent developments, a bank's relationship with a fintech company may or may not involve critical bank activities, depending on a number of factors. It is up to each bank's board and management to identify the critical activities of the bank and the third-party relationships related to these critical activities.

Jurisdictions with TPRM guidelines have one common characteristic: They are broad by design and for good reason.

Any overtly prescriptive regulation is counter-intuitive to achieving effective TPRM.

As the bar is constantly being raised on what constitutes an effective TPRM strategy – not least because of the ever-changing regulatory environment as well as the variety of relationships with vendors – banks must be given room to fully respond to all possible scenarios and quickly transition into crisis management mode. ✱

■ *Julia Chong is a Singapore-based writer and researcher.*

---

locations. If significant external events or internal change is identified, a reassessment of the third-party relationship may be warranted.

### STEP 8 ▸ IMPLEMENT REGULAR REPORTING

Ongoing reporting may include scorecards and key risk indicators (KRIs) at the relationship level as well as KRIs and key performance indicators (KPIs) at the portfolio level.

This perspective can expose concentration risk, including multiple relationships with a single third party or over-reliance, through multiple third parties, on individual fourth parties. Portfolio-level KRIs can reveal aggregate risk, total cost of relationship, and compliance monitoring. KPIs illuminate how well the third-party risk management programme is operating in terms of the responsiveness of third parties and the timeliness of assessments and reassessments.

### STEP 9 ▸ DEPLOY TECHNOLOGY

The most mature third-party risk management programmes implement comprehensive technological solutions that assist with workflow, reporting, and monitoring, including: data and metadata capture from multiple sources | extensive and flexible reporting and analysis capabilities | a centralised document repository | workflow automation tools with reminders | integration with other systems.

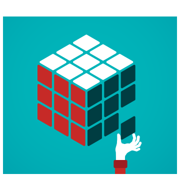
### STEP 10 ▸ TRACK PROGRAMME PERFORMANCE & QUALITY

It is critical to maintain visibility into its performance by measuring risk reduction and quality assurance. This involves monitoring KPIs and addressing issues before they negatively affect programme efficacy. Verify that assessments and reassessments are occurring in a timely and efficient manner, that third parties and internal staff are responsive in addressing concerns, and that adverse events or internal and external changes are reported appropriately. The third-party risk management team should investigate negative trends in any of these areas.

**SOURCE** Adapted with permission from Crowe LLP.

# FRTB: MAKING THE MOST OF A LIFELINE

*Are banks transforming at the required pace to meet the extended 2022 deadline?*



**Instead, FIs should strive to meet both the letter and spirit of FRTB; an infinitely more troublesome but strategic endeavour that could ultimately offset banks' cost in this monumental exercise.**

Fundamental Review of the Trading Book (FRTB), the standard that forms part of what's commonly referred to as 'Basel IV', is nothing short of a paradigm shift in the global market-risk regulatory framework. In the EU, FRTB will be implemented as part of the Revised Capital Requirements Regulation.

While FRTB's impact will vary between jurisdictions and banks of differing sizes, the market is currently seeing a long phase-in period. The new first-time adoption is set for 1 January 2022 for both implementation and regulatory reportings, with phase-in arrangements for various aspects to extend well into 2027.

The standard had previously been slated for implementation on 1 January 2019 and this extension is nothing short of a lifeline for global financial institutions (FIs) – one that should be used wisely if banks intend to capitalise on potential gains of this rigorous new standard.

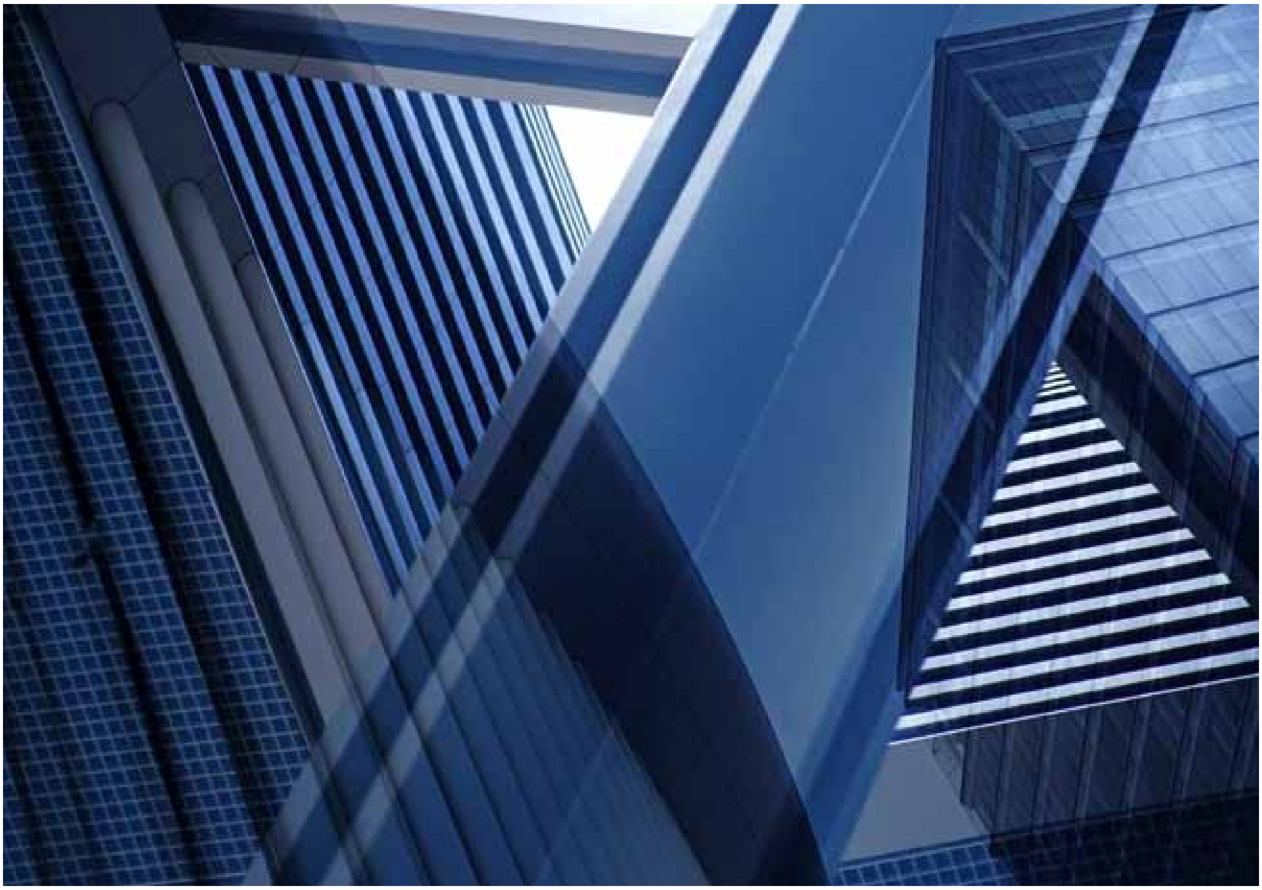
## CAPTURE GAINS

Just as all roads lead to Rome, so too can banks meet FRTB requirements in a multitude of ways. What separates the good from great will be seen in the efficiencies and transformations gained from this sector-wide endeavour.

By fulfilling the letter of law, i.e. what is expressly laid out in FRTB, banks will have complied with the regulation but missed out on two things: meaningful change and the opportunity to reap efficiencies within this new regiment.

Instead, FIs should strive to meet both the letter and spirit of FRTB; an infinitely more troublesome but strategic endeavour that could ultimately offset banks' cost in this monumental exercise.

In its April 2018 research, *FRTB Reloaded: The Need for a Fundamental*



*Revamp of Trading-Risk Infrastructure,* McKinsey & Company succinctly described this broader strategic goal as "implementing FRTB in a smart way" and wrote: "Banks that choose this path will capture benefits in capital efficiency, cost savings, and operational simplification."

The global consultancy goes a step further to project that the benefits derived from tackling the deeper challenges of FRTB can mitigate banks' estimated 3-percentage-point reduction in ROE arising from compliance.

**BACKGROUND**

In January 2016, the Basel Committee on Banking Supervision (BCBS) issued a revised standard, *Minimum Capital Requirements for Market Risk,* to address what it described as "major structural shortcomings of the Basel II market-risk framework".

Its key features include:

- a more objective boundary between the trading book and banking book;
- greater coherence of risk measure using the Expected Shortfall (ES) method instead of Value-at-Risk (VaR) to capture 'tail risk' and maintain adequate capital during times of market stress;
- the revised standardised approach (SA) to serve as a floor for the internal models approach (IMA); and
- incorporation of the risk of market illiquidity.

On 7 December 2017, after monitoring the pace of implementation of the market risk standard as well as its impact on banks' market risk requirements, the BCBS' oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS), endorsed the final aspects to outstanding Basel III regulatory reforms except FRTB which was deferred to 2022.

This move was not unexpected and much of it had already been built in to market expectations. In Asia Pacific specifically, regulators had already anticipated and made clear their positions on FRTB as they negotiated within the larger 'Basel IV' reforms.

*Reuters,* in a news report dated 5 July 2017, wrote that the Monetary Authority of Singapore (MAS) had told lenders it will delay by a year the implementation of global rules designed to rein in trading risks. An MAS spokeswoman said the regulator remains committed to a full implementation of Basel III reforms but was not rigidly adhering to a timeline.

"In determining the implementation timeline, MAS will consider factors such as the state of global implementation guidance, the industry's readiness

It is one of the most wide-ranging regulations for banks in recent years and its implications should not be underestimated. Aside from the complexity of operationalising the trading book changes, many are still wrapping their heads around a strategic approach to this new market-risk framework.

and implementation progress in other jurisdictions," she said in a statement.

Prior to the abovementioned report, the Hong Kong Monetary Authority and the Australian Prudential Regulation Authority had previously announced FRTB implementation dates of no earlier than January 2020 and 2021, respectively.

A person familiar with the committee's workings said to *Reuters* that capital for trading books is a small proportion of a bank's total buffer and therefore a delay in FRTB does not materially affect the bigger capital picture for the banking sector.

**BEEFING UP**

The ball is now in the courts of the respective jurisdictions to not only prepare themselves for the new 'go-live' of this market-risk framework, but also to draft all the necessary laws to accommodate it within their respective national legislatures. No mean feat to be accomplished in the next three years.

The BCBS press statement, which includes reference to FRTB as part of its announcement on the larger 'Basel IV' rules, clearly states: "GHOS members also reaffirmed their expectation of full, timely, and consistent implementation of all elements of this package, including the minimum capital requirements for market risk. The standards agreed by GHOS constitute minimum standards. As such, jurisdictions may elect to adopt more conservative standards."

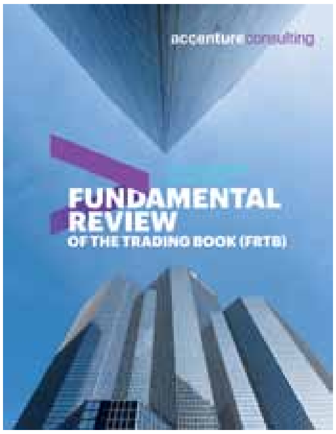
"Moreover, jurisdictions will be considered compliant with the Basel framework if they do not implement any of the internally modelled approaches and instead implement the standardised approaches."

For banks, this is a chance to beef up their systems and architecture to meet the new requirements. The BCBS is currently addressing specific outstanding issues with global financial institutions (FIs), the latest iteration being its March 2018 consultative document, *Revisions to the Minimum Capital Requirements for Market Risk,* with input received from over 40 FIs.

It is one of the most wide-ranging regulations for banks in recent years and its implications should not be underestimated. Aside from the complexity of operationalising the trading book changes, many are still wrapping their heads around a strategic approach to this new market-risk framework.

Although the BCBS paper does not explicitly state the infrastructure upgrades that must occur to accommodate FRTB, in many ways compliance will require a strategic realignment of a bank's business, finance and risk functions, especially with regard to consistent application of 'golden sources' of data throughout.

On this score, Europe, vide MiFID II, is




already ahead on design and build of a unified trusted data source for the market by establishing trade repositories which cull real transaction-based data from banks within its jurisdiction.

But for most others, getting to alignment or establishing best-in-class technical knowledge of FRTB implementation – P&L attrition, non-modellable risk factors, IMA vs. SA business case, shift from VaR to ES – is a work in progress. What's often overlooked is the importance of data integrity underpinning every function under the new market risk framework, from modelling to reporting.

**What's often overlooked is the importance of data integrity underpinning every function under the new market risk framework, from modelling to reporting.**

## INFRASTRUCTURE INVESTMENT

This 'smart way' or effective FRTB implementation is invariably linked to optimal data management – the cultivation and maintenance for consistent, standardised data – and looks into all aspects of its management, i.e. taxonomy, governance, quality, sourcing, aggregation methods, infrastructure deployment.

These recommended steps in Accenture Consulting's 2017 paper, *FRTB: From Theory to Action,* hold true for banks intending to optimise outcome of FRTB deployment, going beyond compliance and seeking to unlock cost and capital efficiencies:

### 1 IDENTIFY A CONSISTENT SET OF SENSITIVITIES

This involves a systematic approach to bucketing sensitivities or risk exposures for individual risk classes. Maintain the same sensitivities definition across the front office and risk management teams by having a common taxonomy for both. Establish standard data taxonomies for attributes across risk classes and sensitivities and use throughout the organisation. Ideally, sensitivities are calculated only once by a golden source calculator then utilised throughout the bank.

### 2 DEFINE A CENTRALISED ARCHITECTURE FOR SOURCING RISK DATA

Set up a central repository for all risk sensitivities. This repository would receive data from different golden sources for risk sensitivities and it should be stored and organised by risk class, bucket, tenor, and risk factor, respectively. A favoured practice is to establish a unified feed format from multiple sources that can be established via data-feed service level agreements from data providers. This should also withstand internal and external audit approvals.

### 3 MANAGE IMA RISK FACTORS AND LIQUIDITY HORIZONS

Individuate criteria and indicators for distinguishing between modellable and non-modellable risk factors. Participate in data pooling initiatives within the industry or subscribe to third-party vendors for obtaining real prices, but be mindful of potential manipulation. Develop activities for the control of data for each desk instead of the legal entity as a whole, with flexibility in switching to SA approach in case of rejection by supervisors. Structure computations to easily manage the inclusion/exclusion of the desk considered eligible/ineligible for the internal model. This can bring about reduced capital charges due to IMA.

### 4 PLAN FOR P&L ATTRIBUTION

Define the factors governing the portfolio that is to be considered for P&L attribution and communication protocols to different departments involved, such as finance, for integrating desks which are eligible for IMA. Revise the report system for risk management based on the outcome of the backtesting. This will allow for effective deployment of IMA to compute capital charges resulting in successful P&L attrition tests.

### 5 MANAGE SA RISK SENSITIVITIES

Document existing data that is useful for sensitivity management from the front office systems. Periodically update the dataset to confirm the existing risk factors and identify any new risk factors impacting the models. This will correct sensitivity gaps and update SA calculators.

### 6 IMPROVE MARKET DATA PROCESS FOR DATA QUALITY MANAGEMENT

Integrate IT processes which warn/alert users of data issues in the repository. Signal to both users and affected functions the data issues and eventual delays to improve management of the activities.

### 7 SEEK TECHNOLOGY SYNERGIES WITH OTHER REGULATORY INITIATIVES

Leverage the existing infrastructure for supporting FRTB and avoid duplicative work by identifying synergies with other strategic regulatory initiatives such as BCBS 239 (Principles for effective risk data aggregation and risk reporting) and the Uncleared Margin Regulation. If they are in the middle of implementation, make sure that the technology solutions for different regulatory programmes are supporting FRTB requirements as well. Maintaining strong data lineage in this manner results in cost savings and permits compliance across all regulatory regimes.

Now that the clock's been reset on FRTB, how is your bank making the most of this lifeline? ✱

■ *Kannan Agarwal is an assistant researcher currently engaged in economic and financial modelling with a social enterprise.*