Gurdeep Singh, CB, Deputy Chairman of AICB's Chief Credit Officers' Forum and Regional Head of Retail Risk at CIMB Bank Bhd

Risk & Reward

BANKING INSIGHT

IDEAS FOR LEADERS | DECEMBER 2024

PP 17327/05/2013(032407)

Trustless

Banking's next iteration calls for a radical shift within.

A PUBLICATION OF

AICB

ASIAN INSTITUTE OF CHARTERED BANKERS

ISSN 2231-8267

Financial Fragmentation: How Geopolitical Risks Are Altering Global Payment Flows

CHECK POINT: ASEAN TAXONOMY VERSION 3

DATA GOVERNANCE AT THE FORE

Frankfurt School of Finance & Management

German Excellence. Global Relevance.

ASIAN BANKING SCHOOL

ABS | Professional Certification

CERTIFIED EXPERT IN BIODIVERSITY FINANCE

AICB CPD HOURS

1 CPD hour for each hour of study time, up to a maximum of 20 CPD hours per course

This online learning course is designed to deepen your understanding of risks associated with biodiversity loss and empower you with the knowledge and tools needed to support the preservation of Earth's diverse ecosystems as financial actors.

- Two intakes per year (March and September)
- 6 months course with 3 - 4 hours of self-study per week
- Consists of 5 mandatory units, which build upon each other
- Content delivered by leaders and experts in Sustainable Finance
- Equips you with the knowledge to advance UN SDGs
- Internationally recognised certificate

HRD CORP CLAIMABLE

MYCO ID: 10001377930

Visit: www.asianbankingschool.com • Email: training@asianbankingschool.com

Scan QR Code for more information

This programme equips you with knowledge to advance the following SDGs:

Editor's Note

Side Step or Quick Step

One of banking's greatest virtues is its clear, straight-talking approach when dealing with difficult situations. That is exactly what we need to steer the industry in anticipation of headwinds that look set to dominate 2025.

With a record of over 70 countries having gone to the polls in 2024, the most crucial was the outcome of the US elections with president-elect Donald J Trump returning for a second term with a stronger Republican mandate in controlling the trifecta of the White House and both chambers of Congress.

David Coleman, Vice President, Chief Risk Officer, European Bank for Reconstruction and Development, who most recently spoke to *Chartered Banker*, the magazine of our UK partner, the Chartered Banker Institute, said: "We have instability, volatility, and the absence of predictability…All of these are macro risks."

"If we want to have an environment within which people invest their money and banks can be certain that businesses are going to survive and therefore be able to pay them back, not only do we need to have relatively low volatility and instability, but that stability has to extend to the legally sound regions as well."

With geopolitical turbulence and the tussle to deregulate the sector becoming more prominent, it is timely that our exclusive Chartered Banker interview this issue feature a thoroughbred risk professional, Gurdeep Singh, CB, Deputy Chairman of AICB's Chief Credit Officers' Forum and Regional Head of Retail Risk at CIMB Bank Bhd for his insights on the rewards that come with getting the strategy right.

With the growing whispers of deregulation and emerging innovations in decentralised finance (DeFi), our cover story, *Trustless*, by Angela SP Yap delves into the concept of 'trustlessness', a key concept in DeFi, and explores the complexities of trust in technology and proffers a different power-sharing model when it comes to banking's relationship with DeFi.

Organisational strength is explored in a different dimension, that of cybersecurity, in *The Human Firewall: Cyber Resilience Starts with Organisational Culture,* by Christophe Barel, Managing Director APAC at FS-ISAC. By fostering a culture of security awareness, enforcing ongoing training, and implementing proactive risk management, institutions can beef up technical firewalls by shoring up on their human defences first.

The rise of cryptocurrencies is also presenting a unique set of challenges. In *Never to be Bedfellows?*, the article zooms in on Custodia Bank's legal battle to secure a master account with the US Federal Reserve and raises practical challenges about crypto innovation, its coexistence with traditional banking, and whether it compromises financial stability.

Resilience in the banking industry requires a multifaceted approach – one that blends collaboration, strong organisational culture, and innovative strategies to address both current and emerging risks. These complex yet critical challenges were tackled at the recent International Conference on Financial Crime and Terrorism Financing Masterclass 2024, hosted by the Institute in Kuala Lumpur from 19 to 20 August 2024. With immersive and experiential sessions that combined our best-in-class talents with over 40 global and regional experts, the two-day event spurred intense discussions and knowledge transfers on transnational financial crime, ultimate beneficial ownership, and enhanced frameworks to strengthen detection through inter-agency cooperation.

With headwinds already here, side-stepping is not an option. It's clear that quick steps delivered head-on are banking's best bet to secure its future.

Here's to our resilience as we embrace the challenges of 2025! ✱

The Editor

"If we want to have an environment within which people invest their money and banks can be certain that businesses are going to survive and therefore be able to pay them back, **NOT ONLY DO WE NEED TO HAVE RELATIVELY LOW VOLATILITY AND INSTABILITY, BUT THAT STABILITY HAS TO EXTEND TO THE LEGALLY SOUND REGIONS AS WELL."**

AICB BANKINGINSIGHT

Editor - Edward Ling
Assistant Editor - Shireen Kandiah
Editorial Assistant - Felicia Song
Writers - Angela SP Yap, Julia Chong, Kannan Agarwal, Dr Amanda Salter, Liam Lisu

PUBLISHER
Asian Institute of Chartered Bankers
197701004872 (35880-P)
(formerly known as
Institut Bank-Bank Malaysia)
Levels 11 & 12, Bangunan AICB
10 Jalan Dato' Onn
50480 Kuala Lumpur, Malaysia
Tel +603 2602 6833
Email enquiries@aicb.org.my

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

PRINTER
Empress Print Sdn Bhd
No. 33, Jalan PBS 14/8
Taman Bukit Serdang, Seksyen 14
43300 Seri Kembangan
Selangor Darul Ehsan
Tel +603 8959 9233

WE WANT TO HEAR WHAT YOU HAVE TO SAY ON BANKING INSIGHT.

Why not drop us a line now?
enquiries@aicb.org.my

Visit us online at our website
www.aicb.org.my

CONTENTS | DECEMBER 2024

COVER STORY

EXCLUSIVE

Future-fit Talent

Malaysia's first Future Skills Framework (FSF) was launched on 22 July 2024 at Sasana Kijang, constituting an important step in pursuit of the Financial Sector Blueprint 2022-2026, which calls for a whole-of-industry and national approach to address the pressing challenges in the financial sector.

A comprehensive and customisable talent planning tool, this finance-sector-led initiative aligns industry's future needs with capacity-building programmes for the acquisition of vital skills.

Spearheaded by the Asian Institute of Chartered Bankers (the Institute) in collaboration with the Islamic Banking and Finance Institute Malaysia and the Asian Institute of Insurance, the event was officiated by Datuk Abdul Rasheed Ghaffour, FCB, Governor of Bank Negara Malaysia; and Yang Berhormat Steven Sim Chee Keong, Minister of Human Resources, Malaysia.

The Governor, in his keynote address, said: "[T]raditional strategies for recruitment and sourcing – such as through conventional graduate pathways – might no longer be the best way to attract talent with the right skills. We have seen organisations increasingly embracing a 'skills first' approach in attracting, hiring and developing talent. This prioritises individual skills and competencies, irrespective of how they are acquired. And with technology, organisations can equip their employees with tailored skills based on business needs as and when they are needed and in a more cost-effective way. Further, by adopting a 'skills first' strategy, employers can open opportunities for more people with the right skills mix to join the industry to drive organisational success."

Edward Ling, the Institute's Chief Executive said, "As Malaysia aims for a 35% skilled workforce by 2030, the FSF marks a pivotal step in advancing a future-ready financial sector workforce. "AICB is proud to lead this initiative, reflecting our commitment to addressing the industry's evolving needs, setting high standards for skills mastery, and fostering continuous learning for the sector's growth and professional excellence."

FSF has identified

159
relevant job roles

157
in-demand skills over the next three years

Nearly 1,000
capacity-building programmes for access

(From left to right): Edward Ling, Chief Executive, AICB; Datuk Yvonne Chia, FCB, AICB Council Member, Independent Non-executive Chairman, Standard Chartered Bank Malaysia Berhad; Dato' Mohd Muazzam Mohamed, Group CEO, Bank Islam Malaysia Berhad; Datuk Abdul Rasheed Ghaffour, FCB, Governor, Bank Negara Malaysia; YB Steven Sim Chee Keong, Minister of Human Resources, Malaysia; Tan Sri Azman Hashim, FCB, Chairman, AICB; Antony Lee, CEO, AIG Malaysia Insurance Berhad; Paul Low, CEO, Asian Institute of Insurance; Yusry Yusoff, CEO, Islamic Banking and Finance Institute Malaysia; and Thomas Mathew, Group CEO, TalentCorp Malaysia Berhad, at the official launch of the FSF on 22 July 2024.

Responsible AI

A Reach too Far?

The 2024 *Kyndryl Readiness Report* reveals that while 76% of businesses are investing in traditional artificial intelligence (AI) and machine learning, only 42% see a positive return on investment. Additionally, 86% of leaders believe their AI implementation is best-in-class, yet 71% feel their IT infrastructure is not fully prepared for AI deployment.

According to Effendi Azmi Hashim, Managing Director of Kyndryl Malaysia and Indonesia, banks looking to embark on their generative AI (gen AI) journey should consider the following critical factors:

+ **Trusted Data Source:** Input will always determine output – and before banks can trust insights provided by a new technology like gen AI, they must trust the data that is informing them. The reliability and scalability of gen AI hinge on a strong data foundation. Banks must prioritise data privacy, quality, and a comprehensive data strategy.
+ **Use Case Examination:** It is essential for banks to investigate how they should adopt gen AI to drive efficiencies, deliver greater value and achieve business goals. Without a clear understanding of the purpose behind AI implementation, the technology may not yield the desired outcomes.
+ **LLMOps Frameworks:** To derive value from gen AI in a cost-effective manner, it is crucial for banks to incorporate Large Language Model Operations (LLMOps) frameworks into a larger data and AI architecture.
+ **Trusted Partnerships:** As banks modernise with new technologies, IT estates become more complex and challenging. Collaborating with trusted and experienced partners can help them better manage their IT environments and achieve business goals.
+ **Skill Sets and Expertise:** Equally important is the need for banks to upskill their workforce and build specialised talent in areas like data engineering, platform design, and responsible AI practices.

GROUNDBREAKING USD120 BILLION PLEDGE FOR CLIMATE ACTION

At the 29th United Nations Climate Change Conference (COP29) in Baku, Azerbaijan, this November, multilateral development banks (MDBs) made a groundbreaking pledge to significantly boost climate finance for low- and middle-income countries. As part of a broader strategy to meet global climate goals, MDBs aim to mobilise up to USD120 billion annually by 2030, with USD42 billion dedicated to adaptation efforts and USD65 billion from private sector contributions. This funding will support both climate adaptation and mitigation in the most vulnerable regions of the world, generating long-term environmental and economic benefits for countries at greatest risk.

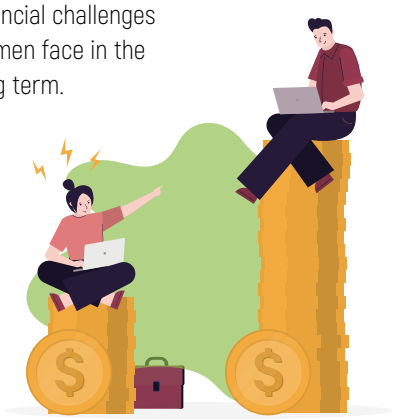
In addition to their financial commitment at COP29, the MDBs introduced several initiatives to track and accelerate global progress on climate action. Key among these is the push for a strong New Collective Quantified Goal on Climate Finance (NCQG), aimed at guiding countries in fulfilling their targets under the Paris Agreement. They also unveiled the Common Approach to Measuring Climate Results, a framework designed to link global mitigation and adaptation efforts with tangible MDB outcomes, and introduced the Country Platforms for Climate Action initiative, which emphasises their support for closer collaboration between host countries, MDBs, donors, and the private sector.

By the end of 2024, the MDBs will have already surpassed their initial goals set in 2019, with a 25% increase in direct climate finance and a doubling of mobilisation climate efforts. This progress is helping to accelerate the launch of new platforms and forge deeper partnerships with organisations like the International Monetary Fund to maximise impact. This collective commitment marks a pivotal moment for the MDBs in driving systemic change and fostering a more resilient global future.

EUROPE GOES SLOW ON PAY EQUITY

The EU's annual 'Equal Pay Day' is a symbolic day that highlights the gender pay within the Union. The event, which took place this year on 15 November, indicates that slight progress has been made over the years as their women are still comparatively underpaid compared to their male counterparts. On average, women are being paid approximately 13% less, meaning that they only earn the equivalent of 10.5 months salary for every 12 months a man is paid. Over the past decade, progress in closing this gap has been slow, with only a 3-percentage point reduction since 2014.

In a joint statement issued by the EU's Vice-President Věra Jourová and Commissioners Nicolas Schmit and Helena Dalli, attention was drawn towards the continued gender segregation of the labour market where women are disproportionately overrepresented in low-paying sectors such as caregiving and part-time roles are prevalent. Career interruptions and reduced working hours, particularly following maternity leave, further exacerbate the financial challenges women face in the long term.



The statement further called upon EU member states to fully implement the Pay Transparency Directive, an initiative that promotes pay transparency, grants job-seekers access to pay information, requires gender pay gap reporting, and introduces joint pay assessments. Such directives aim, therefore, to create a more level playing field by ensuring that women have the same opportunities for fair compensation as their male colleagues.

Unbanked Segment Shows Upside in Blockchain Collaborations

Blockchain technology is playing a pivotal role in advancing financial inclusion across Asia using a collaborative tripartite model comprising fintech, banks, and regulators.

Addressing the long-standing challenges that banks face when serving the unbanked seems to finally be paying off for the traditionally unprofitable sector – the unbanked market has been considered high-risk and low-reward, with banks struggling to assess creditworthiness due to their limited or unreliable data. Blockchain technology is offering a more efficient and effective solution.

Henry Choi, Head of Group Retail TMRW at UOB Bank, in an interview with *The Banker* published on 7 October, reported that over 50% of the bank's total customer base in the Association of Southeast Asian Nations were acquired through the in-house digital platform and digital engagement has also jumped to 70% from 58% since 2022 to the present.

HSBC India has partnered with microfinance institution Satin Creditcare Network Ltd to automate the process of disbursing fully digital loans, utilising blockchains to ensure transparent and efficient payment processing at every stage. The application programming interface (API) that powers their blockchain-based solution extends credit to three million economically active women in rural and semi-urban regions and small- and medium-enterprises keen on transitioning to green using its INR120 crore (RM63 million) securitisation deal with HSBC India. The API democratises access to financial products through improved data analytics, making it easier for banks to identify and serve the right customer segments, thereby reducing the risks typically associated with lending to underserved populations.

Risk & Reward

Reporting by the Banking Insight Editorial Team

Keeping banks relevant in the face of tomorrow's turbulence.

As emerging financial technologies reshape the banking landscape, ***GURDEEP SINGH, CB, DEPUTY CHAIRMAN OF AICB's CHIEF CREDIT OFFICERS' FORUM AND REGIONAL HEAD OF RETAIL RISK AT CIMB BANK BHD***, weighs in on the challenges and opportunities that have shaped his perspective as a risk professional, how these values resonate with markets, and why he believes banks continue to be a force for good in society.

Q ***Given your illustrious career in banking, what have been some of the highlights that have kept you in the sector?***

In my banking career of 20 years, I have worked in two banks across two countries, and have seen two major economic crises. Considering, banking was never my career aspiration at the start of my tertiary education, it has been an interesting journey so far.

The best learning experiences in risk management are usually during a crisis. From a risk management perspective, it was an extremely challenging and satisfying experience navigating through the Covid-19 pandemic. Helping our borrowers during the pandemic, while safeguarding the bank, was a fulfilling experience, especially given that the events unfolding at the time were unprecedented. It helped emphasise the vital role that banks play in advancing the customers' needs and society's as well as in fostering greater economic empowerment.

Professionally it has been a satisfying journey – from learning the nitty-gritty of retail risk management at the beginning of my career to being in a position where I can shape things and influence decisions while adapting to new trends. Along the way, I have had numerous learning opportunities to enhance my technical skills to help me do a better job and adapt to new technologies as the banking industry evolves. I have also had the privilege of working under visionary leaders and excellent colleagues.

In the last 20 years, as the banking industry has evolved, so has the regulatory landscape; forcing banks to adapt to remain competitive. Banking is again at the precipice of change, with digital challengers coming in to compete with traditional banks. I continue to do my part to ensure CIMB Bank remains competitive in this changing landscape. I am pleased that the learning opportunities continue, ensuring that things do not get mundane.

One thing which has remained constant throughout my career is that banks continue to

be a force for good and are vital for the community at large.

Q As Deputy Chairman of the AICB Chief Credit Officers' Forum, how do you see the Institute pivoting in its role to strengthen and equip credit professionals for the decade ahead?

Continuous lifelong learning is the only way to keep up with current trends and helps an individual to be present and current. In this regard, AICB offers a wide array of programmes to ensure the banking workforce in Malaysia is constantly being upskilled and prepared to handle the challenges of the future. AICB has updated and revamped its programmes and curricula to meet the needs of the banking industry. The Institute will continue to play a critical role in keeping the banking talent up to global standards, to ensure the Malaysian banking sector stays robust and resilient.

The programmes range from basic courses to advanced programmes like the Chartered Banker, catering to the needs of those who are at the beginning of their banking careers, as well as those who have a considerable amount of experience in the industry. This also helps to overcome the talent shortage seen in the industry.

Apart from the various programmes, the AICB, as the coordinator of various industry forums – such as the Chief Risk Officers' forum, Chief Credit Officers' forum, Chief Information Security Officers' forum – brings together bankers to discuss common concerns and issues as well as emerging trends in the banking industry. These forums also facilitate discussions with the central bank on key concerns, and seek clarification on various regulatory guidelines. Additionally, external experts are brought in to share ideas about new trends and themes in banking, including consultants brought in to share best practices around climate risk management, advance analytics, and other core issues.

Advancements in **COMPUTING TECHNOLOGIES HAVE LED TO MAXIMISING THE POTENTIAL OF THIS DATA.** AI or machine-learning models are being leveraged to improve risk management capabilities. This trend will continue as banks continue to digitise processes and gather more data points to better understand and analyse customer behavioural patterns.

The Institute will continue to play a pivotal role in the improvement of the banking industry in Malaysia.

Q What do you predict to be the next three big trends in the risk and compliance sector?

AI-powered risk analytics will continue to expand rapidly. Data is the currency of 21st century, and banks are sitting on a treasure trove of data which has not been fully utilised yet.

Advancements in computing technologies have led to maximising the potential of this data. AI or machine-learning models are being leveraged to improve risk management capabilities. This trend will continue as banks continue to digitise processes and gather more data points to better understand and analyse customer behavioural patterns.

As banks work towards hyper-personalisation of banking services, risk management plays a crucial role to help banks achieve this goal, i.e. by leveraging all available data and capabilities to analyse the data and creating a risk profile of every individual customer.

Along with this, adoption of generative artificial intelligence (Gen AI) will also gather pace; Gen AI has huge potential to which the banking industry can tap in order to extract higher cost efficiencies by leveraging on these technological innovations. Gen AI expertise will become the de facto expectation of the workforce, akin to what

happened 20 to 25 years back when the use of computers picked up in banking – it will not be a 'good to have' skill set; rather it is a 'must have' skill set.

Cybersecurity risks will continue to rise. As banks deploy more technology, gather and store more data, they need to invest more to manage cybersecurity risks. Criminal elements are also evolving to be more sophisticated and leveraging new technologies to exploit vulnerabilities. AI-driven cyberattacks can exploit vulnerabilities in real time. AI tools like deepfake will enhance phishing attacks, allowing for highly customised and convincing scams/hoaxes. Autonomous malware can be created and deployed that evolves without human input, making detection and safeguarding much more difficult. Interconnectivity of systems will impact banks with issues which perpetuate outside of the banking industry, exposing them significantly. Reliance on third-party vendors exponentially increases this risk, as the whole ecosystem is only as strong as its weakest link. Higher standards of cybersecurity will have to be enforced upon vendors who provide services to banks.

Staying on the AI track, the third trend I foresee is also along similar lines. Banks continuously face pressure to comply with evolving global anti-money laundering and counter-terrorism financing regulations. Banks are expected to use advanced tools to identify and monitor suspicious activity, making real-time detection critical. Banks are turning to AI-driven analytics and machine learning to help them automatically flag and detect suspicious transactions, reducing manual effort and boosting accuracy and efficiency. Again, the abundance of available data will help automate real-time suspicious transaction detection, reduce false positives, boosting efficiency and improving throughput.

Q Whilst banks are seeing tremendous growth and challenges on the horizon, they are experiencing a shortage of talent to fill these future roles. Your thoughts on what is needed to recruit future talent, especially in technically demanding roles such as risk.

With the emergence of fintech firms and digital banks, traditional banks are seeing higher attrition as well as difficulty in attracting new talent. Ensuring an employee experience and work culture that is on par with what tech and fintech firms have to offer will be critical to closing the banking talent gap.

Banks play a critical role in our society and need to highlight their existence as a 'force of good for society'. This will resonate with the next generation of workforce. Young professionals rely heavily on technology and in a socially and culturally aware world, a more inclusive vision of the banking industry is required in order to attract and retain future talent. Employee well-being is also a key consideration for the younger generation to decide on a potential employer.

Banks need to expand their internship programmes, to give the next generation of workforce an exposure to working in a bank so that they will remain interested in banking as a career of choice. At the core, a banking career continues to be an attractive proposition; the non-monetary aspect and experience of working in a bank needs to be enhanced to address the needs of the next generation of workforce.

Additionally, training and upskilling opportunities, faster career advancement, career mobility will ensure banks remain attractive as potential employers.

Q As 2024 draws to a close, what would be on your wish list for banking in the coming year?

Malaysia may encounter challenges from heightened geopolitical tensions and policy uncertainty following the US election, which could potentially disrupt global trade flows and amplify global inflationary pressures. Against this backdrop, economic stability is top of my wish list for next year. I hope the downside risks do not materialise and that the Malaysian, ASEAN and global economies stay robust and resilient in 2025. ✱

TRUSTLESS

By Angela SP Yap

Banking's next iteration calls for a radical shift within.

What is trust?

In an industry which draws much of its value from an intangible like trust, it is a question that doesn't get asked often or deeply enough.

Basel III's emphasis on capital adequacy, stress tests, and liquidity thresholds were devised in a post-2008 world to restore trust in banking after the global financial crisis. Close to two decades later, is this framework sufficiently relevant to tackle the challenges that have emerged since?

Today, innovations in decentralised finance or DeFi – financial services that are performed with no centralised authority – are challenging the status quo of traditional banking. The growing use of blockchain-based technologies for lending, investing, and trading has created a seismic shift that is edging out trusted third-party authorities like financial institutions in favour of trust through technological consensus.

In commonspeak, we are moving from 'trust' to 'trustlessness'; with trust in the financial system now being substituted for automated verification processes in the blockchain. Generative artificial intelligence (GenAI), machine learning (ML), smart contracts – these are touted as a cut above traditional banking. Are they?

MY CODE IS MY BOND

In a 2022 speech at the Eurofi Financial Forum, Pablo Hernández de Cos, then Chair of the Basel Committee on Banking Supervision, said: "A trustful and trusted banking system also depends on a scaffolding of regulatory safeguards, including with regard to conduct, safety and soundness, and market integrity.

"Why do I mention all of this? A narrative accompanying some of the emerging streams of financial innovation is centred around the concept of 'trustlessness'. This is often touted as a superior and more efficient model than today's system of banking, allowing individuals to transact in a quasi-pseudonymous manner, with trust being substituted by automated verification mechanisms. 'Trust me, I'm a coder' is almost a mantra in this world.

"While such a vision may be conceptually appealing to some, it falls short of providing the robustness, seriousness, and societal benefits from regulations, supervision, and the rule of law. A trust-free banking system would essentially require society to place its faith in a set of codes and complex models, which we know from history can be subject to errors and model risk. Moreover, advances in financial technology bring with them greater risks to banks' operational and cyber resilience. Breaches in such areas could potentially weaken the fabric of trust in banking.

"Just as few would be willing to board an airplane that does not meet regulatory standards and that has not been inspected by qualified supervisors, I suspect that not many individuals would want to deposit their money in a banking system void of any regulatory and supervisory safeguards."

This is in response to failures at Silicon Valley Bank and Signature Bank last year, digital players that relied on blockchain-based infrastructures to power their real-time cryptocurrency payments network. An instrumental figure in the Basel III framework, Hernández de Cos is expected to follow through with measures to enhance banking liquidity regulations when he takes over as General Manager at the Bank of International Settlements in July 2025.

But is tougher regulation in a climate of unprecedented innovation the only option on the table?

THE COGNITIVE MISER

One of the few who view this differently is Yan Teng, Assistant Professor at the Shanghai Artificial Intelligence Laboratory and PhD candidate at the Ethics and Philosophy of Technology Sector at Delft University of Technology in the Netherlands. His article, *What Does it Mean to Trust Blockchain Technology?,* argues that to characterise our interactions with blockchain technology as 'trustless' isn't just misleading, but factually inaccurate.

He attributes the misnomer to a phenomenon in behavioural science known as 'the cognitive miser', a term coined by

Decoding Trust

Existing research argues that the use of the original blockchain does not eradicate trust. Instead, it enables a shift of trust from third-party authorities, such as banks and governments, to the systems' algorithms, the network's stakeholders, and the underlying economic mechanisms enabled by the blockchains' performances.

Whether there is a need for technology trust depends not only on the practical interest of using a particular technology but also on the extent to which the trustor knows about the technology.

In order to circumvent the risks involved in trusting blockchains, let us look at what elements of blockchain-based systems are potential targets of users' trust.

From a user-centred perspective, trust is still embedded in all blockchain-based interactions. A systematic way to define and understand users' trust in the blockchain is shown in **Figure 1**.

The user-centred blockchain trust framework (BTF), indicated by the dotted-line box, is based on a blockchain engineering framework (BEF) which was first outlined by Notheisen, Hawlitschek, and Weinhardt in 2017.

By mapping the two frameworks side by side, it creates a common approach for understanding the BTF's layers/types of trust and how it relates to elements in the BEF's blockchain-based platform:

The BTF comprises the following four layers

Environment layer. This contains the economic mechanisms that enable the actions in all other layers.

Infrastructure layer. A protocol layer comprising the basic elements of the blockchain infrastructure and the devices running the virtual machine. This trust layer comprises the trust that users have in (a) the developers' collective ability to write and verify the code and (b) where mining is involved, the integrity of the miners to maintain and not manipulate the integrity of the network.

Application layer. As this layer is controlled by participants who deploy the code for application purposes such as smart contracts (digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met), users must trust the application designers.

Agent layer. Governed by the rules and applications set by the previous layers, human and artificial agents (such as bots) interact in two ways: (a) if the system is a closed ecosystem, it can be trusted to fully perform its functions; (b) if the system needs to be bound to external services and interfaces to perform its functions, it pushes the trust issue to the third-party authorities, such as exchanges and online markets.

The framework assists by

- systematically structuring the elements of blockchain-based systems that invite users' trust;
- providing a way for developers and users to reflect on the actual trustworthiness of these elements when interacting on a blockchain system; and
- identifying a trust element or a combination of trust elements that is/are needed to achieve specific goals using the blockchain system.

Source: Adapted from *What Does It Mean to Trust Blockchain Technology?,* Yan Teng, Metaphilosophy LLC and John Wiley & Sons Ltd, 2023.

social psychologists Susan Fiske and Shelley Taylor, which explains that people tend to think and solve problems in simpler ways that demand less effort, instead of understanding things in depth and with a greater appreciation of its complexities.

The difference in cognitive levels explains why some people consider blockchain technology as 'trustless' whilst others view it as a trusted technology.

"Traditionally," Yan writes, "online interactions between heterogeneous participants are facilitated by third-party authorities, such as financial institutions…As the distributed database technology behind bitcoin, blockchain technology came to prominence as a decentralised solution that relies instead on consensus algorithms and rules to ensure the validity and immutability of transactions processed by the peer-to-peer network. With this sort of decentralised nature, the original blockchain can perform as a virtual institution that users can directly rely upon and interact with, which may

significantly reduce the risk, uncertainty, and cost involved in trusting third parties.

"Although some writers describe blockchain technology as trustless or trust-free, others capture the change of trust enabled by the technology as a shift of trust from third parties to the underlying algorithms.

"While each of the efforts partially capture the idea of how blockchains change the way we trust, they fall short of structuring a relatively complete picture of the blockchain-enabled revolution in trust."

Using his proposed solution, the blockchain trust framework (BTF) outlined in **Figure 1**, Yan posits that rather than a static definition of trust, humans need to change the way we view and place trust in technology – as a dynamic interaction between stakeholders, not a static value.

It makes sense. After all, the levels of

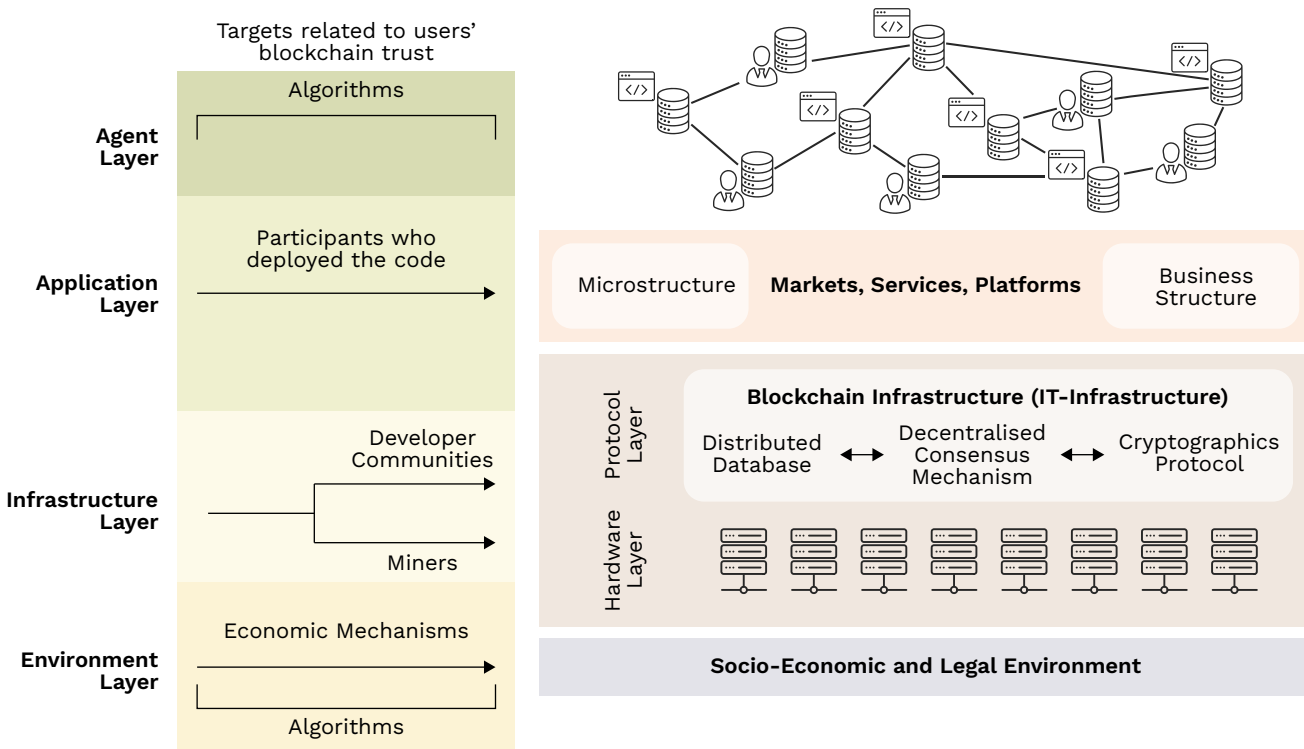


Figure 1 User-centred BTF, based on the BEF proposed by Notheisen, Hawlitschek, and Weinhardt, 2017.

trust in all human-to-human relationships fluctuate from time to time, depending on context, circumstance, and who has greater control. Why shouldn't our trust in technology – especially in smart systems like GenAI and ML – also be seen as a dynamic relationship too?

More than a fancy framework, Yan states that the layers and mechanics of the BTF (see *Decoding Trust* on p.14) should be used "to steer the design and policy-making associated with blockchain implementations, with the aim of indicating directions for developing more trustworthy blockchains and reducing the risk and misplacement of trust."

Rather than a rollback of cutting-edge tech, we should, he argues, develop solutions that make the blockchain a safer, more trustful place through greater decentralisation and robust transparency.

TWO KINGS, ONE CASTLE

In ancient Greece, the city-state of Sparta reached its peak when it was uniquely ruled in what was known as a diarchy – two kings from different dynasties reigned simultaneously in an oligarchic model – which stood in stark contrast to the democratic model of the rival city, Athens.

This exclusive power-sharing feature, examined by Prof George Tridimas' *A Political Economy Perspective of the Constitution of Ancient Sparta: Conflict Resolution, Credibility, and Stability,* led to Sparta's rise. It circumvented intra-elite fighting; redistributed income inequity through this check-and-balance mechanism; which forestalled revolt by the masses and such redistribution was respected by the elite and the masses.

The dual kingship, where both kings were equal in authority and one could not act against the veto of the other, marked a period of stability and prosperity for Sparta, a position which was unrivalled for five centuries until 300 BC.

Imagine if the system of banking was built on such a decentralised power model.

Can banking embrace more 'trustless' technologies like blockchain on equal footing? Could such a novel model achieve a new peak in finance? Will we even contemplate a diarchic model of governance with 'two kings in the castle'?

I hope that this article assists readers in approaching the subject of trust and technology with greater nuance than we have in the past.

Coming up short will have dire consequences. Research indicates that a **10-PERCENTAGE-POINT DIP IN THE SHARE OF TRUST AMONGST PEOPLE IN A JURISDICTION WILL DECREASE** gross domestic product by 0.5 percentage points whilst a decrease in trust by one standard deviation negatively impacts bilateral trade by 90% to 150%.

Coming up short will have dire consequences. Research indicates that a 10-percentage-point dip in the share of trust amongst people in a jurisdiction will decrease gross domestic product by 0.5 percentage points whilst a decrease in trust by one standard deviation negatively impacts bilateral trade by 90% to 150%.

Our approach to governing blockchain technology today will have a ripple effect into every other innovation in the future.

So tell me: can there be two kings in the castle or is there only one seat at the throne? ✱

■ *Angela SP Yap is a multi-award-winning social entrepreneur, author, and financial columnist. She is Director and Founder of Akasaa, a boutique content development and consulting firm. An ex-strategist with Deloitte and former corporate banker, she has also worked in international development with the UNDP and as an elected governor for Amnesty International Malaysia. Angela holds a BSc (Hons) Economics.*

AICB

ASIAN INSTITUTE OF CHARTERED BANKERS

CERTIFICATE IN DIGITAL & AI EVOLUTION IN BANKING (CertDEB)

Demonstrate your mastery of digital, AI, and automated banking technologies, along with the transformative role of Fintech in the financial industry.

Created for bank employees at all levels globally, the Certificate in Digital & AI Evolution in Banking (CertDEB) aims to develop your knowledge of digital, AI, automated banking and the role of Fintech, equipping you with a better appreciation of the scope and evolution of digital and AI transformation in banking, its impact on regulatory, social, and commercial responsibilities, and the accompanying risks and benefits inherent in reliance on technology. Unlock your full potential and seize this great opportunity to enhance your professional development today.

To enrol, please visit www.aicb.org.my

DATA GOVERNANCE AT THE FORE

By Dr Amanda Salter

BALANCING BUSINESS INTEREST IN LIGHT OF THE LATEST LEGISLATIVE TRAJECTORY.

"There ain't nothing safe in this world," as Billy Idol growls in the 1982 hit song *White Wedding*. Most organisations would ruefully agree.

Just recently in October 2024, a malware attack incapacitated India's hill state of Uttarakhand, bringing the government's entire IT infrastructure to a standstill, impacting critical services including the state's Secure Internet Service and the State Wide Area Network. The resulting shutdown of 186 department websites lasted at least days; two weeks later, 32 of those sites were still offline due to outdated systems and expired security software licences.

The attack also revealed crucial gaps in the Uttarakhand government's business continuity plans, leaving officials scrambling to restore critical citizen services and protect sensitive data. In response, a new cybersecurity task force has been proposed together with regular safety audits, mandatory updates for antivirus, and security software at all government offices. A new Chief Security Officer post has been mooted as well as a disaster recovery centre. No doubt, harsh lessons have been learned.

Critics may tut and shake their heads but there can be no righteous stone-throwing by the rest of us glasshouse dwellers. Cybersecurity attacks are ever increasing in sophistication and frequency and similar disasters lie in wait. To appropriate a well-known data security saying, there are only two types of banks: those that know they've been compromised and those that don't. To survive, regulation and legislation are critical in efforts to future-proof the critical sectors like banking.

The following is a quickfire summary of the most interesting changes in data governance and data security laws across Asia Pacific.

WATERSHED LEGISLATION

There are some common legislative trends emerging in the area of data security, such as an increased level of scrutiny around operational resilience and enhanced data breach notification obligations. However, there is still a broad spectrum of disparate legislative requirements coming into force across multiple countries, which is likely to inflate compliance costs for banks.

Some factors at play which may impact any realistic roadmap for compliance could include (on a per-jurisdiction level):

+ size of operational footprint;
+ business strategy and size of the opportunity;
+ number of data subjects;
+ amount of personal data held;
+ data processing activities taking place;
+ number of entrusted parties;
+ penalties, enforcement, and consequences of non-compliance; and
+ maturity of data governance laws.

INDIA
Digital Personal Data Protection Act (DPDPA)

Status: *Passed in August 2023, awaiting implementation via subordinate rules.*

This long-awaited, cross-sector law on personal data protection:

- Applies to the processing of all digital personal data within India, and outside India if it is in connection with services offered to individuals within India.
- Shares some common concepts with Singapore's Personal Data Protection Act (PDPA) 2012, such as an exemption for personal data that is publicly available, such as on social media or other publicly accessible websites.
- Places obligations on data fiduciaries – any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data – to protect personal data, with penalties of up to INR250 crore (approximately RM130 million) for failing to implement reasonable preventative measures against personal data breaches. This is less severe than an earlier legislation in 2022 which proposed a fine of up to INR500 crore.
- Establishes a Data Protection Board, an independent regulator that can set rules, issue penalties, conduct inspections, and impose urgent remedial measures in the event of a

personal data breach.
- Makes data fiduciaries responsible for actions of any data processors they engage.
- Requires timely responses to a data principal's – the natural person to whom the personal data relates, including beneficiaries – request for data access, correction, deletion, and objection.
- Allows data principals to engage registered third party 'consent managers' to administer and enforce their rights, managing consents and data on their behalf. This is a unique concept not covered in some other jurisdictions, such as the UK General Data Protection Regulation (GDPR).
- Requires data principals to be notified of all data breaches, regardless of severity or level of harm caused.

SINGAPORE
Amendments to the Cybersecurity Act (CS Act)

Status: *Passed by Parliament in May 2024, awaiting effective date.*

- Extends the meaning of 'computer system' to include 'virtual computer systems'.
- Clarifies that the owner of such virtual computer systems are the persons who have exclusive control over operations and security.
- Introduces new categories of regulated entities and computer systems to include foundational digital infrastructure (FDI), entities of special cybersecurity interest (ESCI), and systems of temporary cybersecurity concern (STCC). This broadens the earlier coverage of critical information infrastructure (CII) only.
- Increases scope to cover third-party-owned computer systems, not just self-owned.
- Extends coverage to include systems located outside of Singapore.
- Increases regulatory powers of the Cyber Security Agency (CSA) to conduct inspections and require documentation from providers to ensure compliance.
- Requires ESCIs, FDIs, and STCCs to report cybersecurity incidents that lead to a breach of availability, confidentiality, or integrity of the entity's data or that has a significant impact on business operations.

SOUTH KOREA
Amended Enforcement Decree of the Personal Information Protection Act (PIPA)

Status: *Came into effect March 2024.*

- Obliges companies that are processing large amounts of personal data to appoint a Chief Privacy Officer with at least four years of experience in personal information protection.
- Requires data controllers and data processors with annual sales of over KRW1 billion (RM3 million) and more than 10,000 data subjects to have insurance coverage for damages suffered by data subjects as a result of a violation of the PIPA.
- Requires companies to disclose the legal basis for overseas transfers of personal data in privacy policies.

CHINA
Provisions on Regulating and Promoting Cross-border Data Transfers (CBDT Regulations)

Status: *Enacted March 2024 with immediate effect.*

- Provides significant exemptions from the compliance burden of cross-border data transfers under three scenarios, irrespective of data volume:
  - » outbound data transfers necessary for contract signing or performance, such as account opening;
  - » outbound transfers of personal data necessary to safeguard a life, health, or property in the event of an emergency; and
  - » outbound transfers of employee data that are necessary for cross-border human resource management.
- Provides further exemptions based on the volume of individuals affected:
  - » outbound transfers of non-sensitive personal data for less than 100,000 individuals;
  - » outbound transfers of personal data for between 100,000 and one million individuals or sensitive

personal data for fewer than 10,000 individuals are only subject to the China Standard Contractual Clauses filing or certification, rather than a Cyberspace Administration of China (CAC) security assessment; and

» outbound transfers of important data and personal data exceeding one million individuals, or sensitive personal information exceeding 10,000 individuals, requires a CAC security assessment.

CHINA
Regulations on Network Data Security Management

Status: *Passed by the State Council in August 2024, comes into effect January 2025.*

- Covers not only personal data, but also business, industry, and financial data.
- Expands permissible cross-border data transfer mechanisms to include security certification by qualified third parties and transfers necessary for performing mandatory duties. This goes beyond the relaxation of the CBDT Regulations.
- Introduces requirements and best practices for privacy policies, consent forms, and third-party contractual arrangements for data sharing.
- Provides practical details on implementing data portability. Defines prerequisite conditions such as the verified identity of the data subject and technical feasibility of the proposed request.
- Sets penalties for violation of up to RMB50 million (RM30 million) or 5% of last year's turnover, whichever is higher.

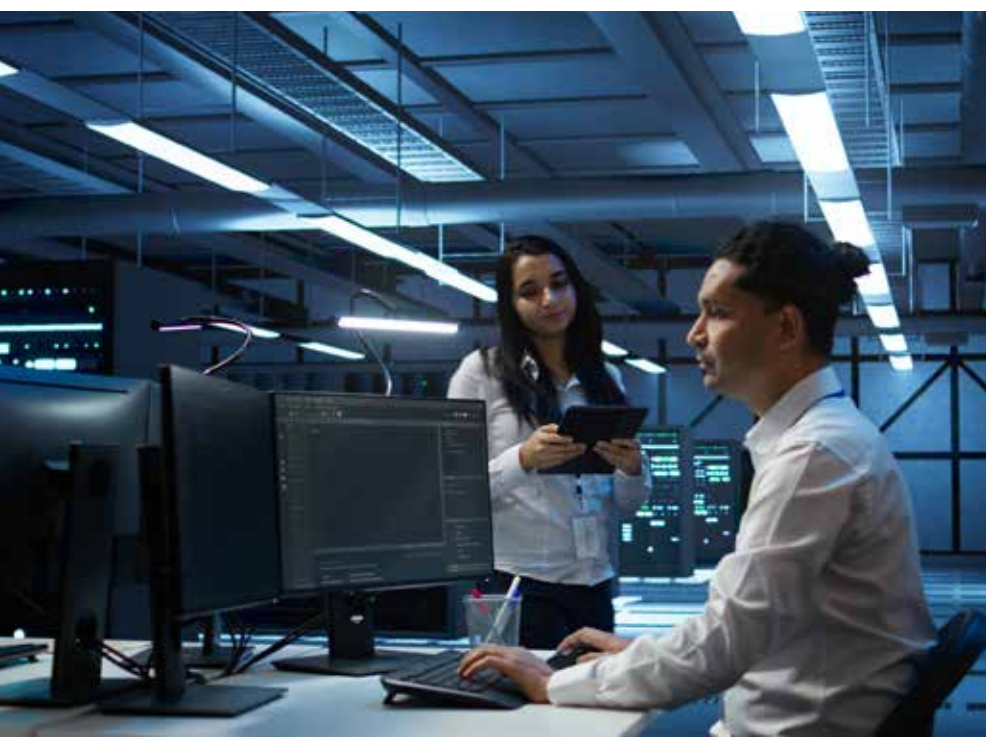
UPCOMING BILLS

There are also four upcoming bills that are of particular relevance to Asia-Pacific banks. The following summaries represent the state of play as at October 2024 and banks will want to stay on top of future developments as the relevant bills progress through the legislative process.

MALAYSIA
Amendments to the PDPA

Status: *Passed by Dewan Negara in July 2024, awaiting royal assent.*

- Aligns the PDPA with international standards, equalising with its Asia-Pacific peers.
- Expands the definition of 'sensitive personal data' to include biometric data.
- Excludes deceased individuals from the definition of 'data subject'.
- Requires data controllers and data processors to appoint a Data Protection Officer.
- Introduces the right of data portability for data subjects, subject to technical feasibility and data compatibility.
- Obliges data processors to comply by taking practical steps to protect personal data. Data processors face new penalties of up to RM1,000,000 and/or up to three years' imprisonment for a violation.
- Increases penalties for breaching the Personal Data Protection Principles to a fine of up to RM1,000,000 and/or up to three years' imprisonment.
- Requires data controllers to notify regulators of personal data breaches and to notify affected data subjects if the breach is likely to cause significant harm. Failure to comply may result in a fine of up to RM250,000 and/or up to two years' imprisonment.
- Revises cross-border data transfer rules to allow outbound transfers to any place that has similar laws to the PDPA or an equivalent level of protection as the PDPA.



SINGAPORE
Digital Infrastructure Act (DIA)

Status: *Announced March 2024, in draft.*

- Covers digital infrastructure that would have a systemic impact on Singapore's economy and society if disrupted, for example data centres and cloud services that support widely-used digital services such as banking and payments.
- Addresses a broader set of resilience risks than the CS Act, from technical system misconfiguration to cooling system failures.

UNITED KINGDOM Digital Information and Smart Data Bill (DISD)

Status: *Announced July 2024, currently in Parliament.*

- Replaces the earlier Data Protection and Digital Information (DPDI) Bill, which was a casualty of the 2024 UK general election.
- Establishes 'smart data schemes', defined as the secure sharing of a customer's data upon their request with third party providers, for example via open banking. This goes beyond the GDPR's data portability rights.
- Establishes digital verification services through secure and trusted digital identity products to support everyday processes such as moving house, purchasing age-restricted goods, and pre-employment checks.
- Proposes a change in the governance model of the Information Commissioner's Office (ICO), the UK's regulatory body for data protection. The ICO is to be given a modern structure with a Chair, Board, and CEO with 'stronger powers'.

UNITED KINGDOM Cyber Security and Resilience Bill

Status: *To be introduced to Parliament in 2025.*

- Intended to update the outdated Network and Information Systems Regulations 2018 and align with the EU Network and Information Security Directive and the upcoming EU Cyber Resilience Act.
- Proposes greater powers for regulators to ensure essential cyber safety measures are implemented and to proactively investigate potential vulnerabilities. This work is to be funded through new cost recovery mechanisms, such as fees collected from regulated organisations.
- Imposes stricter requirements for prompt incident reporting on cyberattacks or ransom demands, to enable identification of attack patterns and effective responses.

HONG KONG Protection of Critical Infrastructure (Computer System) Bill

Status: *Proposed in June 2024, to be introduced to the Legislative Council by end 2024.*

- The jurisdiction's first ever cybersecurity law.
- Applies to designated critical infrastructure operators (CIOs), which includes infrastructure for delivering banking and financial services.
- Applies to critical computer systems (CCSs) that provide essential services or core functions of critical infrastructure.
- Establishes a Commissioner's Office to designate CIOs and CCSs, monitor security threats, assist CIOs in incident response, and investigate non-compliance of CIOs.
- Mandates CIOs to fulfil three types of obligations:
  - » organisation obligations, including setting up a computer system security management unit and informing the Commissioner's Office of material changes to CCSs;
  - » preventative obligations, including conducting security risk assessments and submitting security management plans to the Commissioner's Office; and
  - » incident reporting and response obligations, including participating in security drills, submitting emergency response plans to the Commissioner's Office, and notifying the Commissioner's Office of security incidents impacting CCSs in a timely manner.
- Proposes fines of up to HKD5 million (RM3 million) with additional daily fines for non-compliance.

MOVING FORWARD

Despite these legislative leaps, banks must remain cognisant that the perennial data security challenge for the sector remains unchanged: to achieve a sweet balance between risk mitigation, innovation, and trust.

Multinational banks will want to take a calculated risk-based approach to assess effort and costs for each market, and create a plan for the optimum sequence of compliance with new legislations and rules. ✱

■ *Dr Amanda Salter is a consultant at Akasaa, a publishing and strategic consulting firm. She has delivered award-winning customer experience strategies for the Fortune 500. Dr Salter holds a PhD in Human Centred Web Design; BSc (Hons) Computing Science, First Class; and is a certified member of the UK Market Research Society and Association for Qualitative Research.*

AICB

ASIAN INSTITUTE OF CHARTERED BANKERS

CERTIFICATE IN GREEN AND SUSTAINABLE FINANCE (CGSF)

Develop and demonstrate your knowledge and expertise of green and sustainable finance

The Certificate in Green and Sustainable Finance (CGSF) aims to develop your knowledge, understanding and ability to apply the key principles and core practice of green and sustainable finance, covering key areas of climate change and its impacts, climate risks and emerging environmental and sustainability risks, the evolution of green and sustainable products and services in the banking, investment and insurance sectors, and the role of the finance sector and finance professionals in supporting the transition to a low-carbon world. Unlock your full potential and seize this great opportunity to enhance your professional development today.

To enrol, please visit www.aicb.org.my

CHALLENGES FOR THE BOARDS OF THE FUTURE

By Bob Souster

The future differentiator between 'excellent' and 'good' in organisations.

One of the most important drivers of good corporate governance is leadership. In most banking organisations, the responsibility for leadership lie with the board of directors. It is the directors who decide the organisation's medium- to long-term 'road to travel', commit resources to enable the achievement of organisational goals, as well as putting processes in place to keep the organisation on that road.

The board structures of banks have remained remarkably stable for many years, despite the many upheavals that the banking industry has faced. This article describes the alternative structures that can be adopted, considers some of the challenges that boards may have to face in the future and discusses how this may affect the ways in which boards operate.

The board structures of **BANKS HAVE REMAINED REMARKABLY STABLE FOR MANY YEARS,** despite the many upheavals that the banking industry has faced. This article describes the alternative structures that can be adopted, considers some of the challenges that boards may have to face in the future and discusses how this may affect the ways in which boards operate.

SINGLE-TIER BOARDS

A single-tier board is the most commonly used structure in both private and public limited companies. It is typically made up of **executive directors**, who are full-time employees of the company, and **non-executive directors**, who are appointed as external officers. While executive directors have a contract of service, the non-executive directors are engaged under a contract for service. In most jurisdictions, both types of directors are agents of the shareholders (owners) of the company and have the same legal duties.

Over time, best practices in corporate governance have come to reflect the importance of having proper 'checks and balances' in place to ensure that power and authority at the board and executive levels are not concentrated in too few hands. As a result, many codes of corporate governance now highlight the crucial roles of non-executive directors, with some codes stating that the board of directors should have a majority of independent non-executive directors who can offer an objective view of strategy options as well as providing scrutiny and oversight. Some codes also stress the importance of **segregation of roles**, such as having different persons occupying the role of Chairman of the board and Chief Executive Officer.

TWO-TIER BOARDS

The two-tier board is an alternative structure adopted in several countries, notably in Europe. As the term suggests, a two-tier board has two levels. The **Supervisory Board** sits at the apex of

the organisation and comprises non-executive directors, while the **Operating Board** has responsibility for day-to-day operational matters. In effect, this model separates the executive and non-executive directors, though their roles are similar to those performed in the single-tier model.

STANDING COMMITTEES

As the business operations of large banks, and of larger companies generally, have become more complex, so too have the structures necessary to direct and control them. A typical large bank now has at least four standing committees: Audit Committee; Nominations Committee; Remuneration Committee; Risk Committee. However, some banks have additional committees; some have a Credit Committee to deal with larger or unusual loans, while in recent years some have appointed an Ethics and Standards Committee, reflecting the growing importance of these matters.

THE CHALLENGES OF CHANGE FOR BOARD STRUCTURES

The accepted view is that non-executive directors must play a crucial role in steering the strategies, policies and practices of organisations. But do we expect too much? And are we asking for the impossible going forward?

Non-executive directors are not practising bankers, and very few of those in these roles have direct banking experience. They are expected to exercise independent judgment, but few have an in-depth grasp of the technicalities of banking.

As corporate governance systems have developed, so too has the guidance offered to companies. For example, in some countries the code of corporate governance suggests that at least one member of the Audit Committee should have a detailed understanding of financial management, while one of the international trade associations that represents credit unions states that all members of the board should have a grasp of financial accounts. Likewise, many now acknowledge that it is very difficult for the Risk Committee of a bank to function effectively without at least some members having a comprehensive understanding of risk management and specifically, its importance in asset and liability management.

As corporate governance systems have developed, so too has the guidance offered to companies. For example, in some countries the code of corporate governance suggests that **AT LEAST ONE MEMBER OF THE AUDIT COMMITTEE SHOULD HAVE A DETAILED UNDERSTANDING OF FINANCIAL MANAGEMENT,** while one of the international trade associations that represents credit unions states that all members of the board should have a grasp of financial accounts.

These issues have prompted debates that it may be necessary to broaden the competences of board of directors. Many banks are already exploring fields of operation that were unanticipated only two decades ago. There are exciting opportunities but also daunting threats in decentralised networks and (specifically) blockchain, as well as in artificial intelligence (AI) and machine learning. International commitments to environmental, social and governance (ESG) objectives have already been confirmed in the United Nations' Sustainable Development Goals and the Principles for Responsible Banking. Do all of these developments imply that every bank should have a director who is an expert in AI, another in sustainability, another in cryptocurrencies, and so on?

These questions somewhat miss the point of what a board of directors should do, or what its members should be. A board of directors of a large bank is typically made up of 12 to 18 directors. Boards of smaller banks have fewer members, perhaps between six and nine directors. It is generally acknowledged that a board should be of an 'appropriate' size, with a good balance and mix of knowledge, skills and experience, but once the size of a board exceeds (say) 20 persons, it will become unwieldy and inefficient.

In most banks, the board meets each month, occasionally more often if the need dictates, but its role is strategic, not operational, in nature.

Boards of directors are already guided by experts in their own organisations: the heads of marketing, human resources, compliance and lending are accountable to the board for producing reports, offering policy options and making recommendations for future action. But it is inevitable that boards, as well as the senior executives who put their strategies into practice, will become increasingly dependent on taking expert, usually external, advice when appropriate. However, the directors who ultimately take decisions based on the advice they are given need not, and cannot, be experts in everything.

What these huge changes imply is that the work of a director will continue to evolve. Directors will need to have enough knowledge and understanding, but of more things that are relevant to their companies. To use an analogy, they will have to 'look at the whole forest but not the individual trees in it'. And increasingly, they will have to detach themselves from the details, which is best left to the experts. In fact, one future differentiator between excellent organisations and merely good ones may not just come down to the quality of the board and management, but the calibre of the experts and advisers who support them. ✱

■ *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 has worked extensively on the Chartered Banker MBA programme at Bangor University, Wales, since its inception, serving as both a Module Director and, currently, as a Moderator for 'Ethics, Regulation and Compliance' and 'Financial Institutions' Risk Management.'*

Financial Fragmentation: How Geopolitical Risks Are Altering Global Payment Flows

By Julia Chong

The radical uncertainty of this risk type should not be underestimated.

In this year's *Global Payments Report,* management consulting firm McKinsey estimate that global payments flow in 2023 hit an all-record high of USD1.8 quadrillion with a revenue pool of USD2.4 trillion on the back of 3.4 trillion transactions. This represents a 35% share of total banking revenue and indicates the severe knock-on effects a change in global payment systems can have on the financial system.

UNEQUAL RISKS

The fact that these record numbers come at a time of heightened geopolitical upheaval is cause for concern. Notably, the Russia-Ukraine conflict and deteriorating US-China relations have negatively impacted cross-border investment portfolios and bank credit allocation.

In banking, although the risk function sits squarely under the chief risk officer's purview, the treatment of geopolitical risk is often left out of the equation, or at best, treated as a subjective touchy-feely sort of analysis mostly because it is viewed as an ambiguity compared to other quantified risks under the Basel regime.

Unlike loan default rates or tiered capital allocation rules, financial institutions cannot rely on traditional, quantifiable risk indicators when measuring geopolitical risk. The closest guidance that the Basel Committee on Banking Supervision has

issued is its consultative document on *Guidelines for Counterparty Credit Risk Management* released on 30 April 2024 which states:

"Banks should ensure, at the point of onboarding, that their processes consider and assess non-financial risks as part of the credit risk decision-making process. Banks should also establish an escalation process and clear communication channels for the review of non-financial risks. For instance, banks should appropriately characterise the intersection between CCR (counterparty credit risk) and geopolitical or country risk. This is a process that may benefit from consultation with the legal department at the point of onboarding…These non-quantifiable risks can transform into CCR over the longer term even in cases where no direct impact on the probability of default can be seen."

"Banks should ensure, at the point of onboarding, that **THEIR PROCESSES CONSIDER AND ASSESS NON-FINANCIAL RISKS AS PART OF THE CREDIT RISK DECISION-MAKING PROCESS.** Banks should also establish an escalation process and clear communication channels for the review of non-financial risks."

GEOPOLITICAL RISK DRIVERS	CHARACTERISTIC	TRADITIONAL RISK DRIVERS
LOW. Geopolitical events can emerge unexpectedly and escalate rapidly.	Predictability	**HIGHER.** Economic cycles and market trends can be better modelled with historical data.
HIGH. Involves complex, interconnected relationships between political events, economic impacts and the financial system across countries, regions, and institutions.	Interdependencies	**LOWER.** Generally, more contained within financial systems and less influenced by non-economic events.
DIFFICULT. Cannot be easily quantified or modelled probabilistically due to inherent uncertainty.	Quantification	**EASIER.** Can often be quantified using historical data and probabilistic models (e.g. credit scores, value-at-risk).
HIGH. Characterised by a lack of clear information leading to challenges in defining responses.	Ambiguity	**LOWER.** More data-driven with clearer information available for decision-making.
HIGH. Potential scenarios are diverse and can vary significantly.	Range of outcomes	**LOWER.** Outcomes are generally more predictable within a certain range based on historical patterns.

Table 1 Characteristics of geopolitical and traditional risk drivers
Source: Speech by Claudia Buch, Chair of the Supervisory Board of the European Central Bank, *Global Rifts and Financial Shifts: Supervising Banks in an Era of Geopolitical Instability,* 26 September 2024.

As vague as such advice may seem, geopolitical risk drivers are no less important than traditional risk drivers but because of the differences, as shown in **Table 1,** they should be assessed differently to the other types of risk that currently make up the arsenal of back-office risk calculations.

A BRIDGE TOO FAR

Although geopolitical instability seems a distant occurrence for banks in the Asia-Pacific region, it is imperative that they be on the lookout for future radical shifts in the payments and settlements landscape.

For instance, SWIFT (Society for Worldwide Interbank Financial Telecommunication) is the main messaging network through which international payments are initiated. Although very few banks in the region were directly affected by the sudden ban by SWIFT against Russian banks in 2022, the waves that reverberated throughout Asian financial markets were real.

An immediate circular by the Monetary Authority of Singapore (MAS) to local financial institutions (FIs) cautioned the sector about heightened risks and to take "appropriate measures to manage any legal, reputational, and operational risks arising from the sanctions" imposed on Russia with regard to the ongoing Ukraine conflict.

"FIs should also continue to stay vigilant to any suspicious transactions or flow of funds, and apply enhanced customer due diligence in higher-risk situations," an MAS spokesperson told *Asian Banking & Finance* in response to its queries.

Under such volatile geopolitical circumstances, prudence is warranted.

FRAGMENTED FUTURE

The International Monetary Fund's (IMF) *Global Financial Stability Report* issued in April 2023 highlights: "Financial fragmentation induced by geopolitical tensions could have potentially important implications for global financial stability by affecting the cross-border allocation of capital, international payment systems, and asset prices."

The international funder estimates that a one-standard-deviation increase in geopolitical tensions between an investing and a recipient country, such as the US and China, could reduce cross-border portfolio and bank allocation by about 15%. Other financial stability risks for the global banking sector include a sudden reversal of cross-border credit and investments, increased debt-rollover risks, and higher funding costs for banks.

The international funder estimates that a **ONE-STANDARD-DEVIATION INCREASE IN GEOPOLITICAL TENSIONS BETWEEN AN INVESTING AND A RECIPIENT COUNTRY,** such as the US and China, could reduce cross-border portfolio and bank allocation by about 15%. Other financial stability risks for the global banking sector include a sudden reversal of cross-border credit and investments, increased debt-rollover risks, and higher funding costs for banks.

Across the board, all risk indicators confirm geopolitical tensions are increasing. The latest IMF working paper, *Geopolitical Proximity and the Use of Global Currencies,* published this September, reports that the Geopolitical Risk Index, an aggregate index that measures the number of adverse geopolitical events, has doubled in recent years. The global Trade Policy Uncertainty Index has also reached a historic high due to increased cross-border trade restrictions and foreign investment controls.

The authors, Jakree Koosakul, Longmei Zhang, and Maryam Zia, write: "Accordingly, persistent geopolitical tensions could significantly reshape cross-border capital flows and influence countries' currency preferences vis-à-vis foreign exchange reserves, international payments, and trade invoicing.

"Since the end of World War II, the US dollar has been the dominant currency for international transactions, accounting for more than 60% of the total, followed by the euro and a few other currencies. However, increasing

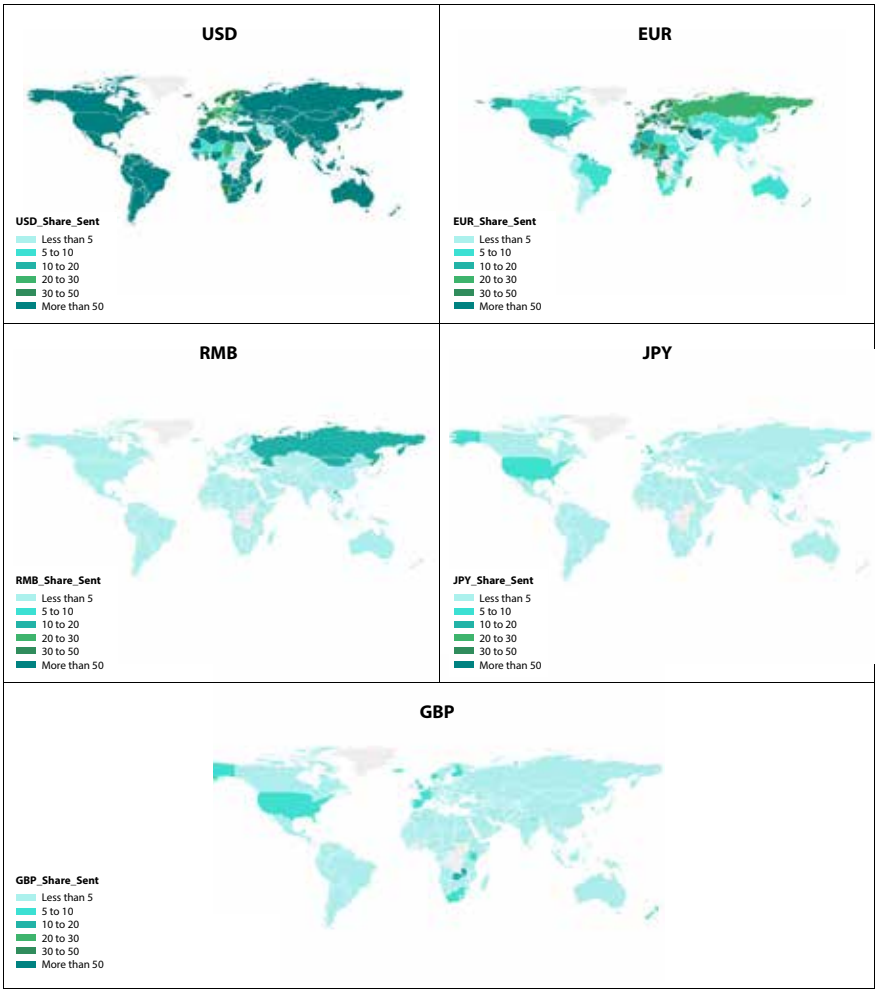


Figure 1 Distribution of SWIFT payments by currency – *Currency share in total SWIFT payments in 2022*
Source: SWIFT and IMF staff estimates.

geopolitical tensions may impact decisions on currency usage and the payment network underlying it. This paper aims to shed light on the extent to which geopolitical factors affect currency usage, along with traditional economic factors, such as trade, financial linkages, and geographical distance."

Examining the IMF's basket of five special drawing rights (SDR) currencies – the US dollar, the euro, the Chinese renminbi, the Japanese yen, and the British pound sterling – and how their use varied with the level of geopolitical tensions, the researchers were able to determine the effect of geopolitical tensions on the use of global currencies in cross-border transactions.

Based on SWIFT data, global currency shares indicate significant regional variations. **Figure 1** shows the extent of use of the five SDR currencies in cross-border payments across regions.

"While the US dollar has broad dominance, accounting for more than half of payments in most regions, the euro plays an eminent role in most of Europe and parts of Africa. The renminbi has gained traction in parts of Asia, such as Mongolia and Laos," the report states.

"Interestingly, the US dollar has a larger presence in China for cross-border payments than the RMB itself. Outside of Japan, the Japanese yen is mainly present in Thailand's cross-border transactions. The British pound is frequently used in Europe and parts of Africa."

Cross-border payment networks used for international settlements have been traditionally US dominated. The most widely used, SWIFT, although headquartered in Belgium, is US controlled. The payment network has often been seen to be used as a tool to achieve US foreign policy objectives. An interview with two of its former executives in 2021 quotes them as saying that, "No bank can afford to lose access to the US payment system. If overseas banks do not comply with US sanctions, the US can simply forbid its banks to process dollar transactions for them."

A NEW INTERNATIONAL PAYMENTS ARCHITECTURE?

In recent times, several alternative payment systems and/or new technological platforms have come to the fore:

> **mBridge:** A blockchain-based platform for real-time, cross-border payments and foreign exchange transactions using central bank digital currencies or CBDCs. This backend payment infrastructure, which reached minimum viable product stage in June 2024, will hook up to existing banking systems. The joint project was

developed between the Bank of International Settlements (BIS) Innovation Hub and a multi-central-bank collaboration which includes the Bank of Thailand, the Central Bank of the United Arab Emirates, the Digital Currency Institute of the People's Bank of China, the Hong Kong Monetary Authority, Saudi Central Bank, and other observing central banks. On 31 October 2024, the BIS announced that it was backing out of mBridge after four years of involvement, following concerns that the payment network could be used to evade sanctions.

- **BRICS Bridge:** A new cross-border digital payment and settlement system based on distributed ledger technology (DLT), was formally announced following the BRICS+ meetings in Kazan, Russia this October. Earlier this year, BRICS expanded its membership from the original five members — Brazil, Russia, India, China, and South Africa — to include Iran, the United Arab Emirates, Ethiopia and Egypt. An accompanying press release announced the coalition's aim to use "local currencies by BRICS countries and their trading partners in financial transactions. We encourage the strengthening of the BRICS correspondent banking network and the promotion of local currency settlement under the voluntary and non-binding BRICS Cross-border Payments Initiative."
- **Cross-border Interbank Payments System (CIPS):** Launched by the People's Bank of China, this real-time gross settlement system clears and settles in renminbi and is considered a direct alternative to western clearinghouses. As at October 2024, the CIPS network comprised 160 direct participants and 1,413 indirect participants (mainly in Asia) – a fair way off from the extensive SWIFT network. It should be noted that CIPS itself still runs on the SWIFT system for cross-border financial messaging.

Although the current global payment architecture is not even close to a shift in the status quo, the increasing prominence of alternative systems and platforms is something that banks should have on their radar at all times. The IMF recommends that "[P]olicymakers need to be aware of **POTENTIAL FINANCIAL STABILITY RISKS ASSOCIATED WITH A RISE IN GEOPOLITICAL TENSIONS** and devote resources to their identification, quantification, management, and mitigation."

HEDGED RISKS

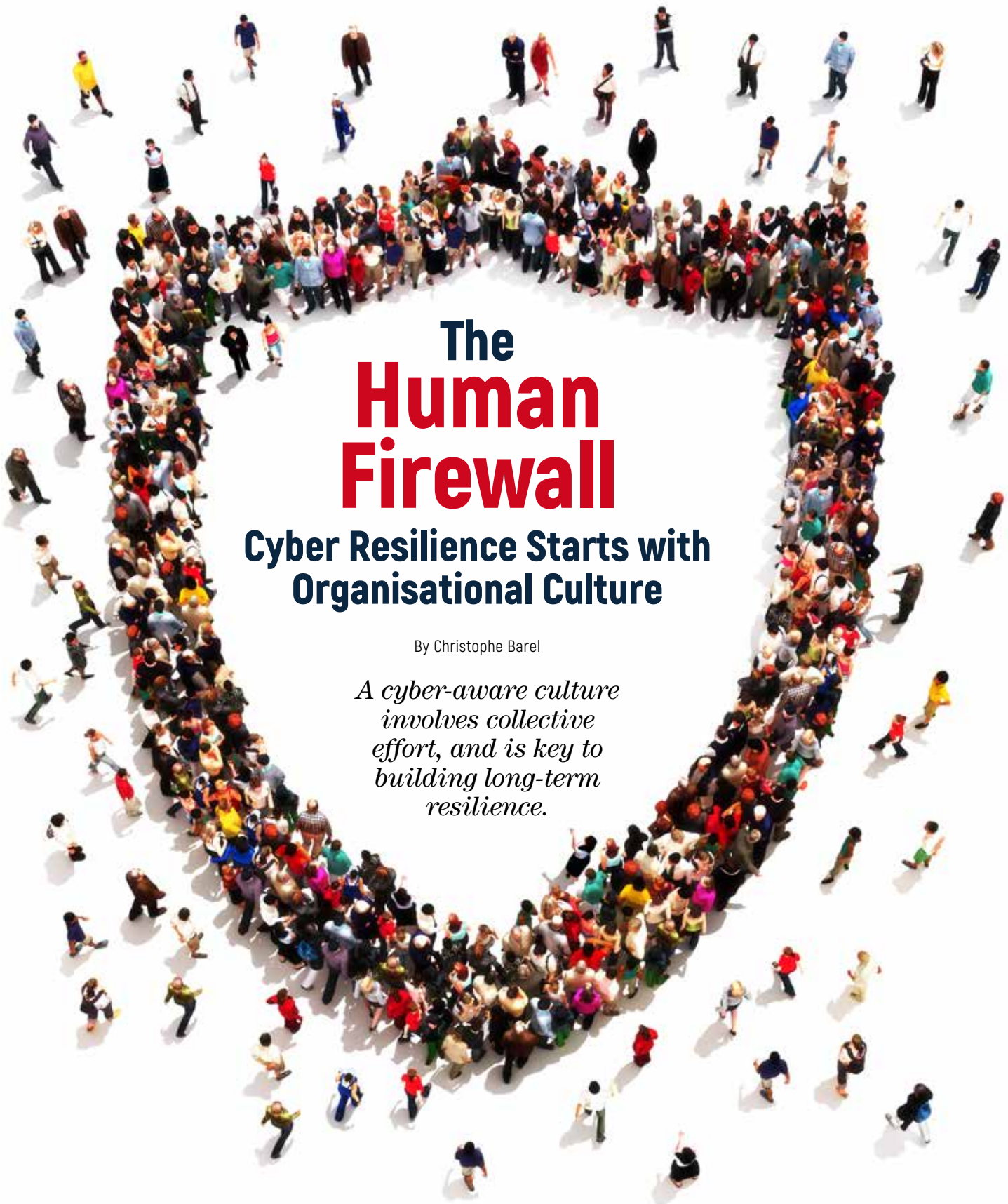
Amid increasing sanctions and escalating tensions, these growing alternatives for the financial sector signal a change in tides as countries and blocs move (albeit slowly) towards de-dollarisation.

Although the current global payment architecture is not even close to a shift in the status quo, the increasing prominence of alternative systems and platforms is something that banks should have on their radar at all times. The IMF recommends that "[P]olicymakers need to be aware of potential financial stability risks associated with a rise in geopolitical tensions and devote resources to their identification, quantification, management, and mitigation."

Navigating the future calls for every bank to ensure its risk management framework robustly accounts for direct and indirect geopolitical risks.

A fine line to tread, for some more than others. ✱

■ *Julia Chong is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*



The Human Firewall

Cyber Resilience Starts with Organisational Culture

By Christophe Barel

A cyber-aware culture involves collective effort, and is key to building long-term resilience.

In today's landscape, where cyberthreats are constantly evolving, the resilience of financial institutions require more than just state-of-the-art technology, which alone cannot guarantee full protection.

At the heart of an organisation's cyber resilience is its people, who foster a culture that prioritises cyber awareness and hygiene, forming a human firewall essential to robust cybersecurity.

THE CYBER HYGIENE GAP: A STARK REALITY CHECK

Despite today's fraught cyberthreat landscape, many organisations still struggle to implement basic cyber hygiene practices effectively. This gap is often due to a mix of factors: insufficient awareness, where employees and leaders alike may lack a deep understanding of cybersecurity risks; a tendency to overlook best practices due to perceived inconvenience; and the technical limitations that challenge smaller financial institutions or those with lower cyber maturity. These vulnerabilities can leave an organisation exposed to breaches that can have severe consequences.

Within the interconnected financial ecosystem, one institution's cyber resilience can influence the overall risk landscape. This was exemplified by the recent Crowdstrike outage in July this year. Though the outage wasn't the result of a cybercrime, the incident underscored the global financial sector's vulnerability to cybersecurity disruptions. Relying on Crowdstrike's cybersecurity services, institutions worldwide faced massive operational disruptions. The incident led to an estimated USD1.15 billion in losses to the banking sector alone, highlighting the far-reaching consequences of such outages. The incident also exposed critical dependencies on third-party providers, highlighting the urgent need for institutions – and the sector as a whole – to build cyber resilience.

Resilience begins with getting the fundamentals right – yet concerningly, the Cyber Security Agency of Singapore has identified a significant knowledge and experience gap in cybersecurity implementation and basic cyber hygiene as a major barrier for organisations, with 59% of businesses and 56% of non-profits citing it as a key challenge.

The repercussions of this gap – financial losses, reputational damage, and operational disruptions – are too significant to ignore. Therefore, regardless of size or cyber maturity, all financial institutions must prioritise fundamental cyber hygiene practices to enhance their resilience.

THE MISSING LINK: CULTURE AS THE FOUNDATION OF CYBERSECURITY

Even the most advanced cybersecurity strategy can falter if an institution does not foster a robust organisational culture that ingrains cybersecurity into the firm's DNA. This culture must promote a shared understanding that security is a collective responsibility and prioritise cyber awareness and hygiene to ensure the long-term effectiveness of security technologies.

Leadership plays a crucial role in shaping this culture by championing and modelling strong cyber hygiene practices. Employees look to their organisation's leaders to set the tone from the top, with 80% of respondents to a 2024 LogRhythm report believing that cybersecurity leaders and CEOs should be primarily responsible for defending against and responding to cyber incidents. Leaders within the institution should also implement clear cybersecurity policies and procedures and ensure these are communicated clearly and regularly to all employees. Additionally, leaders should provide employees with ongoing cybersecurity training and resources, including phishing and social engineering awareness, data handling best practices, two-factor authentication, and endpoint security.

Employees, in turn, should be equipped with the knowledge and skills needed to recognise and respond to threats through regular training and awareness programmes. This education must go beyond surface-level instructions; it should cultivate a deep understanding of the evolving threat landscape and provide practical tools for recognising and mitigating risks in real time. Creating systems that can detect unusual behaviours and patterns, and gathering intelligence to identify look-alike websites that pose phishing threats will help employees build skills and confidence.

Human decisions play a critical role

in security outcomes, especially as increasingly rampant social engineering tactics like phishing exploit human psychology. According to the Financial Services Information Sharing and Analysis Center's (FS-ISAC) *Navigating Cyber 2024* report, generative AI is expected to fuel a rise in phishing emails and deepfakes, and notes an increasing trend in smishing (SMS phishing) – the use of social engineering through mobile texting and QR code phishing.

In Singapore, the average amount lost per scam was SGD14,503 in 2024, marking a 7.1% increase from the previous year. Most fraud incidents start with social engineering exploits that open breaches in the firm's systems. In the first half of 2024, the most common types of social engineering scams involved e-commerce, job posts, and phishing. Hence, a strong culture of awareness can empower employees to identify and mitigate these threats. This is especially crucial as adversaries increasingly use generative AI to craft sophisticated scams, including deepfake video, audio, and one-on-one communications. Tailored training that addresses the specific risks associated with different roles can further solidify a culture of vigilance.

This rising incidence and sophistication of fraud schemes highlight the need for financial institutions to secure their infrastructure while also focusing on external customer protection. Customers should know how their financial institutions will communicate with them so they can flag irregular messages as potential frauds, and they should be able to report such attempts easily. Ideally, financial services firms should have a process to receive and parse those reports and share them internally. Aggregated shared signals could lead to preventative actions.

A holistic approach is essential, integrating fraud prevention into application development, product design, and service delivery. As part of fostering the sector's collective resilience against disruptions, industry organisations such as FS-ISAC play a leading role through a growing suite of anti-fraud initiatives, including fraud intelligence alerts and reports, coordinating sector-wide efforts to enhance collaboration via intel and data sharing, and law enforcement coordination.

No organisation, regardless of size or resources, can completely prevent all cyberthreats – highlighting the critical importance of building resilience. By integrating best practices into daily operations and **CULTIVATING A STRONG CULTURE OF CYBER AWARENESS**, organisations can create a human firewall that is essential for establishing resilience against ever-evolving cyberthreats.

CYBER HYGIENE AS A DEFAULT STATE OF MIND

Improving an organisation's security posture requires a commitment to everyday practices that reinforce cyber hygiene – these practices should be so ingrained in the organisation's protocols and framework that they almost become second nature.

Training employees on cybersecurity is essential as security is everyone's responsibility. Regular education on protecting systems, especially against phishing scams, is crucial. With the rise of sophisticated scams driven by generative AI, employees should be trained to evaluate behavioural cues and question, "Would this person make that request?"

One effective approach is to conduct regular phishing simulation exercises that can involve emails or messages that mimic real-world phishing attacks. Employees who fall for these scam simulations receive immediate feedback and additional training on recognising phishing signs and other social engineering red flags.

Another important practice is to regularly conduct incident response exercises that simulate various types of cyberattacks in order to build muscle memory. These

exercises should involve cross-departmental teams to ensure everyone understand their role in a real-life incident. Post-exercise reviews and feedback are crucial for refining response strategies. Further, developing various incident response plans tailored to specific attack types is essential. These plans should outline security and recovery steps before, during, and after incidents and must be approved by senior leadership.

Incentivising good cyber hygiene practices can also reinforce a security-focused culture. Recognising and rewarding employees who demonstrate exemplary behaviour underscores the importance of these practices and motivates others to follow suit. Positive reinforcement helps transform good security habits into a natural part of daily routines

Alongside culture, understanding your systems is crucial for defence. An updated inventory of all assets on the network, including physical hardware, remote devices, and cloud applications, should be maintained. Regular software updates with security patches are vital, as these patches fix vulnerabilities and enhance overall security.

FS-ISAC's latest resource on Cyber Fundamentals emphasises the importance of implementing multi-factor authentication (MFA) across all accounts, both internal and external, which can significantly reduce the risk of account compromise.

Additionally, the guidance encourages users to create longer passwords, within reason, to further enhance security. A zero-trust policy, which requires validation for anyone accessing applications and data, combined with the principle of least privilege, ensure users have only the access they need. When paired with MFA, these measures make it much harder for threat actors to infiltrate the system.

RESILIENCE: A MOVING TARGET

Finally, resilience is an ongoing – and never-ending – process, not a one-and-done item that can simply be checked off a list. To ensure continued resilience amid a constantly evolving threat landscape, regularly testing and refining security measures is key. This can include conducting simulated phishing attacks and cyber exercises to assess employee vigilance and running penetration tests to identify and address vulnerabilities before malicious actors can exploit them. These proactive steps can help organisations stay ahead of potential threats and continuously improve their cyber hygiene practices and overall resilience.

No organisation, regardless of size or resources, can completely prevent all cyberthreats – highlighting the critical importance of building resilience. By integrating best practices into daily operations and cultivating a strong culture of cyber awareness, organisations can create a human firewall that is essential for establishing resilience against ever-evolving cyberthreats.

In turn, cultivating a cyber-aware culture requires collective effort. Leadership must set the tone but the vigilance of all employees is crucial to creating a secure environment. By fostering a shared commitment to cybersecurity and empowering employees to make informed decisions, organisations can strengthen their human firewalls and enhance their technical defences. ✱

■ *Christophe Barel is the Managing Director for Asia Pacific at FS-ISAC, the member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve. Founded in 1999, the organisation's real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defence.*

POLYCRISIS? WHAT POLYCRISIS?

By Chartered Banker Institute

'PERMACRISIS' MAY HAVE BEEN COLLINS DICTIONARY'S WORD OF THE YEAR FOR 2022, BUT TODAY, MANY PEOPLE BELIEVE WE ARE IN THE MIDST OF A 'POLYCRISIS'.

In the past 16 years alone, the world has lurched from a global financial crisis to a climate crisis to a pandemic to a cost-of-living crisis. The world has experienced unprecedented weather-based activity – ranging from droughts and floods to devastating wildfires – and has recently felt the very real threats of slow growth, superpower rivalry and a potential third world war.

In late 2022, Columbia scholar and *Financial Times* contributor Adam Tooze popularised the term polycrisis, which describes the simultaneous and overlapping crises facing the world today.

"If you've been feeling confused and as though everything is impacting on you all at the same time" he said, "this is not a personal, private experience. This is actually a collective experience."

The roots of the word polycrisis, according to Tooze, come from an idea that was launched by French theorist Edgar Morin, which was then picked up by Jean-Claude Juncker, the President of the European Commission, in 2016.

Juncker was describing the challenge of governing Europe in the face of the Greek debt catastrophe in the aftermath of the 2008 global crisis, Putin's initial aggression against Ukraine in 2014 and the refugee emergency in Syria triggered by the violent state crackdown in March 2011, which spilled over into Europe, all against the backdrop of Brexit. But it was at the annual meeting of The World Economic Forum in 2023, often referred to as Davos, where, prompted by our most recent combination of worldwide emergencies, the word came to the attention of those within corporate risk.

A FRACTIOUS AND FRAGMENTED WORLD

David Coleman, Vice President, Chief Risk Officer, European Bank for Reconstruction and Development,

states that a huge challenge that we face today is the fact that ironically, despite globalisation in terms of trade, we live in a much more fractious and fragmented world than ever before.

"For a long period of time, there's been hegemony in the greater part of the world. But this seems to be breaking down, and we're seeing a possible retreat from globalisation. This, in turn, means that our supply chain has to be reoriented, which will do damage to prosperity.

"It will also mean that there's less cohesion around tackling the big problems that we need to come together to solve."

Joshua Tucker, Senior Geopolitical Adviser, Kroll, agrees.

"It looks like we're on the precipice of an end of an era and the beginning of new one. This particular period started at the end of the Cold War in the 1990s when we saw the rising dominance of the United States and the West. They were setting general rules of global order in a way that had not been seen during the Cold War, when we had these competing great powers.

"In the background, we had the rise of China. But for a while there, if a nation wanted to be part of the international system, it meant playing ball with the Western order. We saw, for example, the rise of elections around the world because elections were part of the Western order, even if they weren't competitive, free and fair."

On a positive note, however, Tucker explains that a decline in geopolitical conflict occurred over the ensuing three decades. "It didn't go away entirely," he points out. "But compared with what came before, this was a calmer period.

"But now, 30 to 35 years later, we're seeing a fraying of that global order – of Pax Americana. And instead, there are myriad different events happening in lots of different parts of the world – the most obvious being the rise of China, which is sometimes a global rival and sometimes a partner to the United States."

"It looks like we're on the precipice of **AN END OF AN ERA AND THE BEGINNING OF NEW ONE.** This particular period started at the end of the Cold War in the 1990s when we saw the rising dominance of the United States and the West. They were setting general rules of global order in a way that had not been seen during the Cold War, when we had these competing great powers.

Greg Jones, Chief Risk Officer, Europe and Asia Region, TD Securities, points out: "Today, China is the powerhouse that fuels the global economy. If we interfere with that, we know that there will be a great deal of sensitivity across all related markets and what the consequences of that may be.

"But what sits above that is the forthcoming [at the time of print] US election. On an economic and financial scale, this is very much material. Because of course, the US is the primary market and if the election causes a sustainable boom in the US, that's fantastic for global markets. But similarly, if something goes wrong, it'll without a doubt damage them."

LOOKING BEYOND EUROPE

Tucker explains that, today, we're also seeing the US pivoting from thinking just about Europe to having to keep a close eye on much more. "We've seen Russia, which early on in the 1990s looked like it was going to be more of an ally of the West, morphing under Putin and becoming much more of an adversary. And we continue to see the volatility in the Middle Eastern region,

and also in other parts of the world."

He stresses that there are multiple global hotspots that we have to examine in order to see what the future holds and where conflict might break out. He also believes there are, in general, fewer constraints on state actors than we tend to have in more settled periods of time.

"We're in this moment where we have a lower level of certainty around geopolitics than we've had previously," he stresses, using Nagorno-Karabakh as an example. "This was an area of dispute between Azerbaijan and Armenia and it's been frozen under conflict for about 30 years. Then, after Russia invaded Ukraine in 2022 and a conflict broke out in the Middle East in 2024 – right in the middle of all this, Azerbaijan just went in and grabbed the territory."

UK REGULATORS STEP IN

In order to assess the key risk factors currently affecting the financial services sector, TD Securities' Jones looks to some recent economic events. "We had a fantastic reaction to Covid-19 from the central banks," he says. "They truly kept the financial industry and the economies on their feet. But then, as central banks and the regulators started to plan for the reversal of that, we ran straight into the liability-driven investment [LDI] episode, which was, of course, triggered by the Liz Truss and Kwasi Kwarteng mini-budget in September 2022.

"As we all know, this caused a strong market reaction and led to UK regulators looking at securities, financing transactions, fixed income and the market mechanisms that enabled this incident to happen."

Within six months of this occurring, the world witnessed US regional bank distress with the failure of Silicon Valley Bank, Silvergate Bank and Signature Bank in March 2023. Credit Suisse also collapsed at the same time, but the cause was different. "Once again, we had the regulators looking at market structure," recalls Jones. "And their reaction was to revert to cross-sectional reviews, which involves looking across the industry for the highest standards.

"It's common, of course, for banks to be strong in some areas and slightly behind in others. But this doesn't mean that they're risky or that they're not in control. It just means that **THEY'RE POTENTIALLY NOT PREPARED FOR WHAT MIGHT BE AROUND THE CORNER.**"

"It's common, of course, for banks to be strong in some areas and slightly behind in others. But this doesn't mean that they're risky or that they're not in control. It just means that **THEY'RE POTENTIALLY NOT PREPARED FOR WHAT MIGHT BE AROUND THE CORNER.**"

be strong in some areas and slightly behind in others. But this doesn't mean that they're risky or that they're not in control. It just means that they're potentially not prepared for what might be around the corner."

Jones explains that the regulators came under public scrutiny due to the severe nature of these events. "They, quite rightly, started to consolidate, and communication between them improved," he says. "They have colleges, regulatory colleges, where they gather to examine current standards. They look at what they're dissatisfied with and how the markets are operating. And when this happens, it leads to a sharp uplift in terms of expectations."

CLIMATE CHANGE AND DEMOGRAPHIC DEVELOPMENTS

Tucker points out that there are other global developments currently taking place that have geopolitical consequences without necessarily being straight geopolitics themselves.

Number one, he says, is climate change, and then there's the huge question of how that is going to impact the flow of people.

"What is climate change, for example, going to do to people's demand for resources? What is it going to do to the issues of food insecurity? And what is it

going to do to migration?

"Then on top of that, we have demographic developments such as the ageing of Western societies and countries falling under the replacement level of population. How is this going to impact countries' abilities, and what is that going to mean for the resources that different countries have to offer?

"It's a complex world that we're in at the moment," he continues. "When we think about where we currently are, we can look to the hotspots in terms of geopolitical risks. Take Russia's invasion of Ukraine two years ago, and what that did to scramble everything in Europe and scramble everything globally.

"Then in the Middle East, we thought there would be a rapprochement between Israel and Saudi Arabia, but that obviously became disrupted by the activities [Hamas' attacks on Israel] of 7 October and its aftermath."

A SOURCE OF UNCERTAINTY

Tucker continues by explaining that we now have a constant situation in the Middle East that continues to be a source of violence, as well as a source of uncertainty.

"We're never sure if a full-scale war will break out between Israel and Iran or between Hezbollah and Israel and what's going to happen there.

"Then we have the omnipresent question of what's brewing in Southeast Asia, with continuing manoeuvring between China versus the US and its allies. And we're also always looking at how Northeast Asian nations are positioning themselves in that regard.

"And finally, we have signs of growing cooperation between Russia, China, Iran, and North Korea – in various combinations – and the implications of these types of relationships for global stability."

PERMACRISIS OR POLYCRISIS?

So, crucially, does all of this amount to a polycrisis?

Tucker says: "If you're the United States of America right now, you have to watch what's happening in Europe with Russia and you also have to watch what's happening regarding the conflict in the Middle East.

"You're also constantly keeping an eye on what is transpiring in Southeast Asia. That's because if a conflict broke out there, it could be an enormous concern for businesses globally – especially in the middle of the AI revolution with so much of the semiconductor industry and chip production going on in Taiwan.

"There's so much alarming activity in other parts of the world, too," he continues. "We're at a point in geopolitics where there are multiple areas of conflict that have the potential to impact businesses, communities, transport, credit risks and much more."

Take, for example, the recent disruption caused by Houthi rebels launching attacks in the Red Sea – a relatively small-scale intervention by a non-state actor that has caused large-scale disruption in shipping routes.

"It's definitely poly, in the sense that there are a number of events taking place across the globe that contribute to risk and that feed on each other in some ways. But I'm not entirely sure if it amounts to a crisis." ✱

"It's a complex world that we're in at the moment," he continues. "When we think about where we currently are, we can look to the hotspots in terms of geopolitical risks. **TAKE RUSSIA'S INVASION OF UKRAINE TWO YEARS AGO, AND WHAT THAT DID TO SCRAMBLE EVERYTHING IN EUROPE** and scramble everything globally."

■ *This article previously appeared in Issue 2 2024 of Chartered Banker, UK.*

Financial Abuse: When Banks Can Become Agents of Change

By Liam Lisu

How financial institutions can recognise, respond, and prevent the cycle by empowering its victims.

Financial abuse is a pervasive issue that, unlike physical abuse, operates invisibly through bank statements, loan applications, and account transactions. Although still on the fringes of finance, financial abuse is slowly but steadily gaining visibility.

Banks can do more than manage transactions — they can provide lifelines to victims seeking independence, transforming from passive service providers to proactive protectors. By identifying the signs, establishing strong support systems, and partnering with domestic violence organisations, banks can play a crucial role in protecting such vulnerable individuals.

UNDERSTANDING FINANCIAL ABUSE

Who Are the Victims?

Although many view this as an issue that affects women, the reality is that financial abuse can occur in any relationship – husband-wife, mother-child, elder-carer – irrespective of gender. While anyone can fall prey to financial abuse, certain groups are disproportionately affected more than others:

- **Single Parents:** Nearly 48% of single parents surveyed by financial charities StepChange and Gingerbread in 2021 experienced economic abuse, including controlling resources and limiting access to funds.
- **BAME (Black, Asian, Middle-Eastern) Women:** BAME women face higher vulnerability due to systemic barriers, financial dependence, and cultural isolation.
- **People with Disabilities:** Disabilities increase dependency on partners, leaving them more vulnerable to financial exploitation. They also have a harder time accessing higher-paying employment opportunities.

While more common in low-income households, financial abuse also occurs in affluent ones, where wealth may mask financial control.

How Does it Happen?

According to UK charity Surviving Economic Abuse, financial abuse manifests in three ways:

- **Blocked Resources:** Perpetrators may prevent victims from accessing education, employment, benefits, or financial accounts.
- **Controlled Resources:** Victims have their purchasing decisions dictated, are forced to justify expenses, or lose access to shared assets like vehicles or property.
- **Prolonged Exploitation:** Abusers create coerced debts, misuse joint accounts, or damage property to impose long-term financial burdens on victims.

LONG-TERM IMPACT ON VICTIMS

Financial abuse leaves long-lasting scars, often burdening victims with debts that damage credit scores and limit access to housing, loans, and other financial services. Abusers may also sabotage careers or confine victims to low-paying jobs, deepening financial instability.

Because of this, rebuilding independence may be nearly impossible for many victims, especially those without essential documents like formal identification or passports. When children are involved, the impacts also become intergenerational, perpetuating cycles of economic insecurity and dependency.

THE ROLE OF FINANCIAL INSTITUTIONS

With an understanding on how financial abuse can impact victims, the UK Financial Conduct Authority (FCA) created the Vulnerability Guidance Framework below to assist financial institutions to detect,

support, and protect victims:

+ **Establish Secure and Confidential Reporting Mechanisms.** Victims of financial abuse require discrete channels to seek help without fear of exposure or retaliation. Banks can establish private helplines for sensitive disclosures, secure email options, and confidential in-branch consultation spaces. These measures help ensure victims feel supported and protected when reporting abuse.
+ **Train and Empower Banking Staff.** Recognising and addressing financial abuse is vital. Employees must be trained to detect red flags and respond accordingly. These key indicators include:
  - **Behavioural cues:** Nervousness, hesitation, or visible distress, especially if a third party dominates conversations.
  - **Unusual account activity:** Frequent large withdrawals, sudden account closures, or repeated changes to account details.
  - **Verbal hints:** Uncertainty about finances or mentions of imposed restrictions.
  - **Digital signs:** Unauthorised access to accounts or unusual online activity.

  Frameworks like the TEXAS model can also help guide staff in managing such situations:
  - Thank customers for sharing their situation;
  - Explain how information will be handled securely;
  - Seek explicit consent for data use;
  - Ask questions to clarify their needs; and
  - Signpost victims to internal support teams or external organisations.

+ **Collaborate with Domestic Violence Organisations.** Partnering with domestic violence charities equips banks with specialised training, referral pathways to resources like counselling and legal aid, and support for policy development. These collaborations enable banks to empower victims, addressing their immediate needs and helping them regain long-term financial independence.
+ **Protect Customer Confidentiality.** Banks should avoid sending sensitive correspondence to shared addresses or accounts. More secure portals and robust protocols must be employed to block abusers from accessing victims' information, especially in joint account scenarios.
+ **Apply Immediate Practical Measures.** To address any immediate needs of vulnerable customers, banking staff can take mitigating measures for its customers:
  - Setting up independent accounts for victims to regain financial autonomy;
  - Offering emergency financial support to stabilise victims in crisis, such as waiving overdraft fees or providing short-term loans;
  - Restructuring or forgiving loans for victims burdened with debt accrued under duress; and
  - Flexible banking services like budgeting tools or fee waivers for victims to regain financial control.

PROGRESS MONITOR

Some industry bodies and authorities have already issued guidance and recommendations on how banks in different jurisdictions should respond.

In the UK, the charge is led by numerous non-profits and charities such as UK Finance whose work has informed government bodies, namely the FCA whose Guidance on the Fair Treatment of Vulnerable Customers continues to set the standard with the Domestic Abuse Act 2021 as the legislation that empowers the safeguarding of victims. The Act defines economic abuse in domestic situations as "any behaviour that has a substantial adverse effect on an individual's ability to (a) acquire, use or maintain money or other property; or (b) obtain goods and services."

Here, financial abuse is classified as a subset under economic abuse as it specifically relates to control of another person's financial affairs. UK Finance clearly states that financial abuse "may manifest itself as financial and economic control through restriction, exploitation or sabotage – creating dependency and/or insecurity" and legislation covers all persons and relationships.

In Asia Pacific, the Australian Parliamentary Joint Committee on Corporations and Financial Services resolved on 2 April 2024 to commence an inquiry into the financial services regulatory framework in relation to financial abuse; the report is set to be tabled soon. Industry lobbies such as the Financial Advice Association Australia have also put on the record that its financial advisers are "uniquely positioned to detect signs of financial abuse."

However, at a deeper level, tackling financial abuse goes beyond regulatory compliance — it's a societal issue and should be seen as an extension of a bank's corporate social responsibility. In this way, financial institutions have the power to disrupt cycles of dependency and foster more resilient communities by providing safety, support, and a pathway to recovery for those impacted by financial abuse. ✱

■ *Liam Lisu is a content associate with Akasaa, a publishing and strategic consulting firm.*

MEET BNM'S FRAUD DETECTION REQUIREMENTS NOW — AND TOMORROW

Bank Negara Malaysia (BNM) has issued new regulations aimed at keeping the nation's financial system secure. The deadline for meeting these requirements is approaching fast. June 30, 2025, to be exact.

Fortunately, Malaysia's banks don't have to build their own systems or replace existing on-prem legacy systems to meet BNM's regulations. Instead, cloud-based solutions offer ready-to-use solutions to comply with BNM's new rules—both today and in the future.

BNM RULES REQUIRES 'PROACTIVE' FRAUD PREVENTION

Malaysians lost approximately RM1.2 billion to scams last year, as informed in the Dewan Negara, which noted 34,497 online scam cases with estimated losses of RM1.2 billion (*Malay Mail,* 18 March 2024). Meanwhile, three in four Malaysians have encountered a scam at some point. BNM's new regulations aim to reverse this alarming trend.

One of the most striking parts of BNM's new rules for banks requires financial institutions to be "vigilant, adaptive, and proactive" in their fraud and financial crime prevention efforts. By using a term like "proactive" in their new requirement, BNM effectively mandates banks to innovate and stay ahead of new trends.

Here is how BNM requires Malaysia's banks to proactively stop fraud and financial crime.

- **Customer Risk Profiling:** Banks must build granular risk profiles of their customers based on demographics, geography, transaction history, and behavioural patterns.
- **Real-time Fraud Detection:** Once customer risk profiles are built, Malaysian banks must implement real-time fraud risk analysis that is capable of regularly monitoring and blocking suspicious patterns.
- **Prioritised Investigations and Customer Alerts:** Suspicious transactions should be investigated based on set priority levels. Before any flagged transaction is

approved, necessary checks and confirmations must be made with the customer.

> **Enhanced Communication with Customers:** Banks must quickly terminate online sessions where unauthorised activity is suspected, notify customers about using risky apps, clearly communicate when online access is restricted, and require customer consent for detailed device profiling.

With this tight deadline approaching, Malaysian banks must quickly undergo a significant technological transformation.

ENHANCE (DON'T REPLACE) ON-PREM SYSTEMS WITH CLOUD SOLUTIONS

Fortunately, Malaysian banks can meet BNM's requirements without replacing their existing rules-based systems. Here's how cloud technology empowers banks to cut through regulatory complexity to quickly meet BNM's requirements and gain a competitive edge.

- **Compliance is Built In**
  Cloud solutions resigned to adhere to BNM's regulations "out-of-the-box."As a result, banks do not have to adjust or alter their own systems to meet their compliance obligations.
- **Faster Implementation:**
  Unlike on-premise solutions, cloud-based platforms can be deployed rapidly, translating to faster compliance and time-to-value for banks.
- **Focus on Core Business Initiatives:**
  Leveraging pre-built, compliant solutions frees your bank's IT personnel to address critical business initiatives and innovation efforts.

BENEFITS OF CLOUD-BASED SOLUTIONS

Cloud-based solutions are a significant game-changer for Malaysian banks in fraud prevention efforts. These benefits include:

+ **Cost-Effectiveness:** Banks can access cloud-based solutions using a subscription model, eliminating the need to pay expensive upfront costs for traditional hardware and software investments.
+ **Data Security:** Cloud service providers (CSPs) handle sensitive data using a one-way hashing process that conceals, obfuscates, or completely hides personally identifiable information (PII) fields. Encryption can anonymise PII fields in a reversible way.
+ **Scalability:** Cloud solutions are designed to be scalable, enabling banks to seamlessly adapt to new fraud threats, shifts in transaction

volumes, and demands for real-time data analysis. They can also be easily updated to address new regulatory requirements.

+ **Advanced Analytics and Machine Learning:** Access to cutting-edge analytical technology can review large volumes of data in real-time to identify complex fraud patterns and suspicious activity that typically evade traditional methods.
+ **Reduce Fraud Losses:** Significantly reduce financial losses, boosting your bank's bottom line and protecting customer funds and trust.
+ **Fewer False Positives:** Fine-tuned machine learning models to reduce false positives, enhance customers' experiences, and reduce the burden on fraud analysts investigating suspicious activity.
+ **Built-in Responsible AI:** Cloud platforms can assess AI models for potential biases, ensuring fair treatment of all customers. This is particularly important for financial inclusion, as it ensures all customers have equal access to critical services.

Ready-to-go cloud-based solutions give Malaysian banks a significant edge in the fight against fraud. Banks to achieve BNM's compliance and build a more robust, agile, and future-proof security framework for their customers.

TOP 3 CONCERNS ABOUT CLOUD PLATFORMS

While cloud technology can quickly be implemented to address BNM's requirements, it's only natural for banks to have concerns over data privacy and security. Here are some important considerations to take into account.

1. Data Vulnerabilities

Data privacy and security are the backbones of a cloud provider's business. If they do not meet the highest standards, they will lose the trust of banks and their businesses will fail.

Several CSP providers are in operation in Malaysia that meet BNM's strict standards. Amazon Web Services (AWS), for example, hosts several sensitive applications for Malaysian banks in Singapore and are about to open a new state-of-the-art data centre in Malaysia.

> ***Solution:*** *Collaborate with vetted, approved cloud providers that offer a secure infrastructure and extensive security measures across all control systems.*

2. Human Error and Sabotage

Criminal threats are a key concern. But another is human error or deliberate sabotage from an inside or outside party that exposes customer data.

> ***Solution:*** *Regulations like the Personal Data Protection Act (PDPA) mandate strict data protection measures that CSPs follow. These include robust security components like encryption (while resting and in transit), access controls, and intrusion detection systems.*

3. Data Residency

The physical location of stored data is another primary concern—especially in regions with no public cloud provider available. PDPA and other data protection measures can complicate cross-border data transfers, making banks cautious about sending data to providers outside their borders.

> ***Solution:*** *Cloud operators in Malaysia must meet BNM's strict data handling requirements, meaning your bank will not be a pioneer in this effort. Additionally, AWS plans to open a new data centre in Malaysia by the end of the year, meaning banks can keep their data inside Malaysia's borders.*

PARTNER WITH FEEDZAI, A READY-TO-USE CLOUD PROVIDER

BNM's new regulations require Malaysia's banks to take a substantial technological leap forward. Fraud detection systems must handle the massive datasets and real-time analysis necessary for effective fraud prevention.

That's where ready-to-use cloud platforms come into play. Banks can achieve unmatched scalability and elasticity using cloud platforms to meet BNM's requirements using cloud technology. Most importantly, banks can augment existing on-prem solutions instead of replacing them entirely.

Nor do banks have to undertake this journey alone. Malaysian banks can ensure a smooth and secure transition by partnering with a reputable cloud provider with a strong security track record and understanding of the local market. With careful planning, execution roadmap development, and data management strategies in place, banks can effectively leverage cloud technology to implement a robust, agile, and secure future-facing framework.

PRINCIPLES FOR RESPONSIBLE BANKING ACADEMY COURSES

Deepen your understanding of the UN Principles for Responsible Banking and instil meaningful changes in your organisation.

AICB is excited to introduce five unique, leading-edge courses to strengthen your understanding of the UN Principles for Responsible Banking (PRB) and empower you with the expertise to instil meaningful changes at the heart of your organisation. Raise your awareness and knowledge on the concept of sustainability, nature and what it means to be a responsible bank. Develop your understanding in key areas of sustainability and climate change to support your stakeholders in making a positive impact on the environment and society. Learn how to incorporate the PRB in your day-to-day decision-making as a senior banking practitioner. Unlock your full potential and seize this great opportunity to accelerate your learning journey today!

To enrol, please visit www.aicb.org.my

NEVER TO BE BEDFELLOWS?

By Angela SP Yap and Kannan Agarwal

THE DIVIDE BETWEEN CRYPTO AND BANKING PROPER LOOMS LARGER THAN EVER.

On 27 January 2023, the Federal Reserve Board (FRB) rejected the application of Custodia Bank, a special purpose depository institution (SPDI), for the opening of a master account with the Federal Reserve System.

Founded by its CEO and ex-Morgan Chase banker Caitlin Long, Custodia is an uninsured state-chartered bank that provides a regulated path for crypto companies to access banking services. A master account with the Federal Reserve would have given the bank direct access to the national payment and settlement system, cutting out the high costs it currently incurs through intermediary financial institutions because of its SPDI status.

The FRB denied its application based on two grounds: that Custodia's risk management frameworks were not sufficient to address crypto risks; and that it also was involved in "novel and untested crypto activities that include issuing a crypto asset on open, public and/or decentralised networks."

In response, Custodia sued the FRB, contending that the denial was improper and the latter was statutorily compelled to grant it a master account in accordance with US Code Service 248a whereby "all Federal Reserve bank services covered by the fee schedule shall be available to non-member depository institutions…".

Unlike some of the more recent scandals at SPDI/crypto banks whose liquidity profile relied on a funding mix that comprised deposits and short-term borrowings to stay afloat, Long has asserted that Custodia's customer deposits of fiat currency is 100% backed by unencumbered liquid assets, including US currency and Level 1 high-quality liquid assets (HQLA). Under the Basel II Standardised Approach for credit risk, Level 1 HQLA are assigned a 0% risk weight and are the highest quality assets that help banks withstand unexpected cash outflows during market turbulence.

Although some may view Custodia's pursuance of a master account with the Federal Reserve as pedantic, the move is rooted in Long's personal experience with the 2011 cyber theft at online bitcoin exchange Mt. Gox, which still ranks as the largest hack in crypto history estimated at USD350 million in financial losses at the time. In June this year, a class action lawsuit will require the now-defunct exchange to pay creditors to the tune of USD9 billion worth of bitcoin.

Unlike some of the more recent scandals at SPDI/crypto banks whose liquidity profile relied on a **FUNDING MIX THAT COMPRISED DEPOSITS AND SHORT-TERM BORROWINGS TO STAY AFLOAT,** Long has asserted that Custodia's customer deposits of fiat currency is 100% backed by unencumbered liquid assets, including US currency and Level 1 high-quality liquid assets (HQLA).

Custodia's case against the Federal Reserve is rooted in Long's assertion that for financial stability, there needs to be a company that can bridge both crypto and traditional banking within the current system. "Custodia offered a safe, federally-regulated, solvent alternative to the reckless speculators and grifters of crypto that penetrated the US banking system, with disastrous results for some banks," said Long.

The case is seen as a test bed that pushes the boundaries of our current financial system, one in which innovation is forging ahead with no chance for regulators to catch their breath.

CHOKING POINT

Custodia's motion, however, was dismissed by the Federal Court on 29 March 2024 in favour of the FRB.

Long's stoic response: "Custodia actively sought federal regulation, going above and beyond all requirements that apply to traditional banks. The board's denial is unfortunate but consistent with the concerns that Custodia has raised about the Federal Reserve's handling of its applications, an issue we will continue to litigate."

In tandem with the rejection, the regulator gave further pushback by releasing a proposed policy to extend crypto-asset restrictions to uninsured state-chartered banks to put them on a level playing field with national banks and federally insured banks.

This August, the financial institution laid off nine of its 36 employees in a bid to preserve capital. Long said: "Operation Choke Point 2.0 has been devastating for the law-abiding US crypto industry and Custodia Bank has been **HIT HARD DESPITE OUR STRONG RISK MANAGEMENT AND COMPLIANCE TRACK RECORD.** We are right-sizing so we can maintain operations while preserving capital until after Operation Choke Point 2.0 ends or our Fed lawsuit concludes successfully."

The regulatory crackdown has continued under the Biden administration. Nicknamed Operation Choke Point 2.0 – a pointed reference to the Obama-era 'Operation Choke Point' when high-risk businesses such as gambling operators were cut off from mainstream banking access – the colloquialism has gained traction amongst industry players who view it as an attempt to 'choke' them out of accessing mainstream banking services.

Small but high-profile SPDIs like Custodia are unrelentingly pushing back. This August, the financial institution laid off nine of its 36 employees in a bid to preserve capital. Long said: "Operation Choke Point 2.0 has been devastating for the law-abiding US crypto industry and Custodia Bank has been hit hard despite our strong risk management and compliance track record. We are right-sizing so we can maintain operations while preserving capital until after Operation Choke Point 2.0 ends or our Fed lawsuit concludes successfully."

Although Custodia is the first crypto bank to challenge the Fed for its rejection of the opening of a direct account, others in the digital asset industry aren't exactly champing at the bit to become members of this highly regulated sector.

What seems to be the biggest bone of contention isn't so much about the public nature of distributed ledger technology

(DLT) as it is about the permissionless aspect of banks holding cryptoassets like bitcoin or non-fungible tokens and its impact on financial stability.

NOVEL RISKS

The Basel Committee on Banking Supervision's (BCBS) most recent thoughts on the matter are captured in its August 2024 working paper titled *Novel Risks, Mitigants and Uncertainties with Permissionless Distributed Ledger Technologies,* which warns banks of the unique risks posed by technologies in decentralised finance, specifically in relation to cryptoassets which are built on permissionless blockchains.

The latest BCBS research paper outlines known issues, such as the risks of a 'hard fork' in the blockchain, lack of oversight over validators, and lack of settlement finality on many DLTs. It explores potential mitigants within the existing financial system and qualifies that none of these have been deployed under real-life circumstances.

Figure 1 gives a condensed version of the major risks, challenges, and potential mitigants for banks according to the global standard setter.

Figure 1
Source: Adapted from *Novel Risks, Mitigants and Uncertainties with Permissionless Distributed Ledger Technologies,* BCBS, 28 August 2024.

Risks: GOVERNANCE RISK	
Challenges: The decentralised design of permissionless blockchains puts at risk the assets that rest on it in several ways: • **Regulatory and/compliance challenges:** Depending on the degree to which governance is decentralised, banks could struggle to conduct effective due diligence and oversight of third parties. • **Security vulnerabilities:** Exposure to bugs or other types of security vulnerabilities will increase the risk of loss associated with assets that exist on permissionless blockchains. • **Hard forks:** As nodes – computers that store a copy of the blockchain and verify transactions and blocks – must agree on changes and upgrades to the blockchain. When participants cannot agree on updates to the network rules, they may split the blockchain itself, a situation referred to as a 'hard fork'. When a hard fork occurs, assets may be exposed to significant price volatility or loss with knock-on effects in price determination, exposure calculation, and fulfilling capital requirements. • **Off-chain governance:** Many governance mechanisms or procedures of permissionless blockchains occur off-chain, involving various decision-making and coordination mechanisms. It is time consuming and can give rise to suboptimal results, including obscuring conflicts of interest, if the process is rushed in cases of emergencies.	**Potential mitigants:** Business Continuity Planning (BCP) – this involves multiple areas and solutions to reduce governance risks, such as a registry that can be used to recover ownership after disruption or monitoring of permissionless blockchains. For example, in the event of a hard fork, the off-chain records could identify the rightful owner of the assets or the branch of the fork that should be followed. Note that BCP procedures in this sphere, although deployed successfully under experimental environments, have not been stress tested.
Risks: TECHNOLOGY RISK/VULNERABILITY TO VARIOUS TYPES OF ATTACKS	
Challenges: • Permissionless systems might be vulnerable to so-called '51% attacks' when a coordinated effort is put forward to control greater than 50% of the validation nodes thus selecting which, and how, blocks are added to the blockchain. • Banks that participate in permissionless blockchains depend on unknown third parties to process transactions. Malicious actors who carry out a 51% attack would undermine confidence in the accuracy of the ledger, which in turn could affect the value of the assets on it. Permissionless blockchains are subject to a number of other potential attacks, including some unique to permissionless blockchain infrastructure. • Cryptoassets can be used for illicit purposes such as money laundering and terrorism financing due to the different levels of anonymity offered by many blockchains. On a permissionless blockchain, only the data relating to the public sender and recipient address of the transaction are recorded, but there is no association between these addresses and the identity of the private key owners. This means that the authorities may not be able to establish the identity of the two parties of a transaction and, therefore, who is the owner of the asset. • Many permissionless networks also explicitly promote privacy-protecting coins, such as monero.	**Potential mitigants:** • BCP. • Permissioning a subset of node infrastructure – this involves creating known validators that are deemed safe for particular users, such as banks, to interact with.

Risks: LEGAL AND COMPLIANCE RISK

Challenges:

- Permissionless blockchains pseudonymise participants, replacing identifying information with an artificial identifier. This can complicate compliance with KYC, anti-money laundering/countering financing of terrorism (AML/CFT), and sanctions regulations.
- 'Gas fee risk' as validators collect transaction fee payments (referred to as 'gas fees') when a transaction is registered on a blockchain. The fees could be paid to illicit entities conducting validation services pseudo-anonymously.
- In many permissionless DLTs, settlement remains probabilistic, meaning the probability that a transaction could be revoked is always possible, although likely to occur to only a small fraction of blocks. For a variety of reasons, the system may reverse a block containing what participants may have thought was a settled transaction, which gives rise to 'orphaned blocks'.
- Due to this probabilistic settlement feature being inherent in most permissionless blockchains, settlement risk exists even if the relevant legal framework and the blockchain's rules, procedures and contracts have defined the point at which final settlement occurs. The use of probabilistic settlement may still cause misalignment between legal finality and technical settlement which can result in uncertainty about the settlement status of transactions for the parties involved.

Potential mitigants:

- Permissioning a subset of node infrastructure.
- Technology based control over parties and transactions – tokens that parties transact in can be programmed in a way that could control and limit access to ownership or even reverse transactions that have already been processed. Such implementation could take various forms, including denylisting, allowlisting, privacy-preserving identity verification, or empowering a controller.

Risks: PRIVACY, CONFIDENTIALITY, AND CONSUMER PROTECTION

Challenges:

- Some permissionless blockchains provide an open record of transactions that can be viewed by the public. This can raise concerns about privacy and confidentiality and can also enable cyberattacks as less sophisticated users may take fewer precautions and be much easier to identify and track.
- In addition, the ability of nodes to order transactions in a block may run afoul of regulations and consumer protections. For instance, maximal extractable value or MEV – where a block producer manipulates how transactions are ordered, included, or excluded in a block, especially in high-volume smart contract blockchains – is an example of this type of activity.

Potential mitigants:

Technology to address privacy, confidentiality, and consumer protection risks – development is ongoing with potential solutions spanning different methods, from zero-knowledge proofs to fully homomorphic encryption, designed to protect customer information.

Risks: LIQUIDITY RISK AND THE 'PARADOX OF TRANSPARENCY'

Challenges:

- The transparency of permissionless networks could cause or heighten liquidity risks at participating banks.
- Transaction visibility may spur or exacerbate runs on the cryptoassets on the permissionless blockchain and may also act as a coordination device among users whose incentive to withdraw increases when other users do so. For example, recent research indicates that the transparency of a permissionless system exacerbated the run that occurred in the Terra/Luna crash.
- Decentralised, non-contracted validators may be unable to coordinate to mitigate liquidity risk during a stress event by, for example, limiting withdrawals on the network.
- Additionally, many permissionless blockchains have dynamic pricing and during times of stress, the price of transacting itself may increase, and transactions may not be able to be conducted in a timely manner. This can impose a liquidity risk on tokenised assets.

Potential mitigants:

Technology to address liquidity risk – development is ongoing with various solutions being trialled to speed up processing of transactions on the blockchain.

Risks: POLITICAL POLICY AND LEGAL UNCERTAINTY

Challenges:

- A change in laws, regulations, and/or policies could change validator behaviour, sometimes suddenly, in a way that makes the blockchains themselves operationally unstable. For example, jurisdictions could ban or discourage cryptoasset mining, thus reducing the amount of computing power or staked native tokens available to secure the blockchain, temporarily increasing the risk of a 51% attack.
- There is continued uncertainty in some jurisdictions as to how various permissionless cryptoassets will be classified and thus what regulatory regimes will apply.

Potential mitigants:

BCP.

MORE THAN ONE FORK IN THE ROAD

Already, crypto players in advanced markets like the US are proposing that the Securities and Exchange Commission (SEC) adopt a consensus mechanism that would allow it to regulate cryptoassets through simple modifications to existing legislations. Rather than devising new legislation, crypto commentators such as Michael Selig, counsel at a New York-based law firm and expert on crypto regulation, advocate that compromise between innovation and enforcement is the way to go.

Just weeks before the 2024 US presidential elections, Selig writes in an op-ed for cryptocurrency news outlet CoinDesk: "With a change in administration forthcoming, the SEC has an opportunity to institute a hard fork of its own with respect to its approach to crypto regulation. Although legislation is necessary to establish a fulsome legal framework for crypto, the SEC can abandon its regulation-by-enforcement playbook in favour of a pro-innovation regulatory framework that scales to accommodate novel markets."

Now that the next US president has been decided and we await a second Trump presidency, one market observer who spoke with *Banking Insight* commented on the possibility of a potential turn-of-the-tides given the greater role that tech leaders and pro-business billionaires are set to play in the administration. "With Elon [Musk] being a major player and now with [Donald] Trump in, there will be greater pressure to adjust," says the observer.

Logically, the potential workaround which regulators can employ is quite straightforward. Instead of looking at permissionless DLTs, there are several public DLTs that are already permissioned. However, whether they qualify as permissioned under the BCBS' definition is up in the air; there are also risks associated with its low user base. These include the Inter-American Development Bank's LACChain and the European Union's European Blockchain Services Infrastructure.

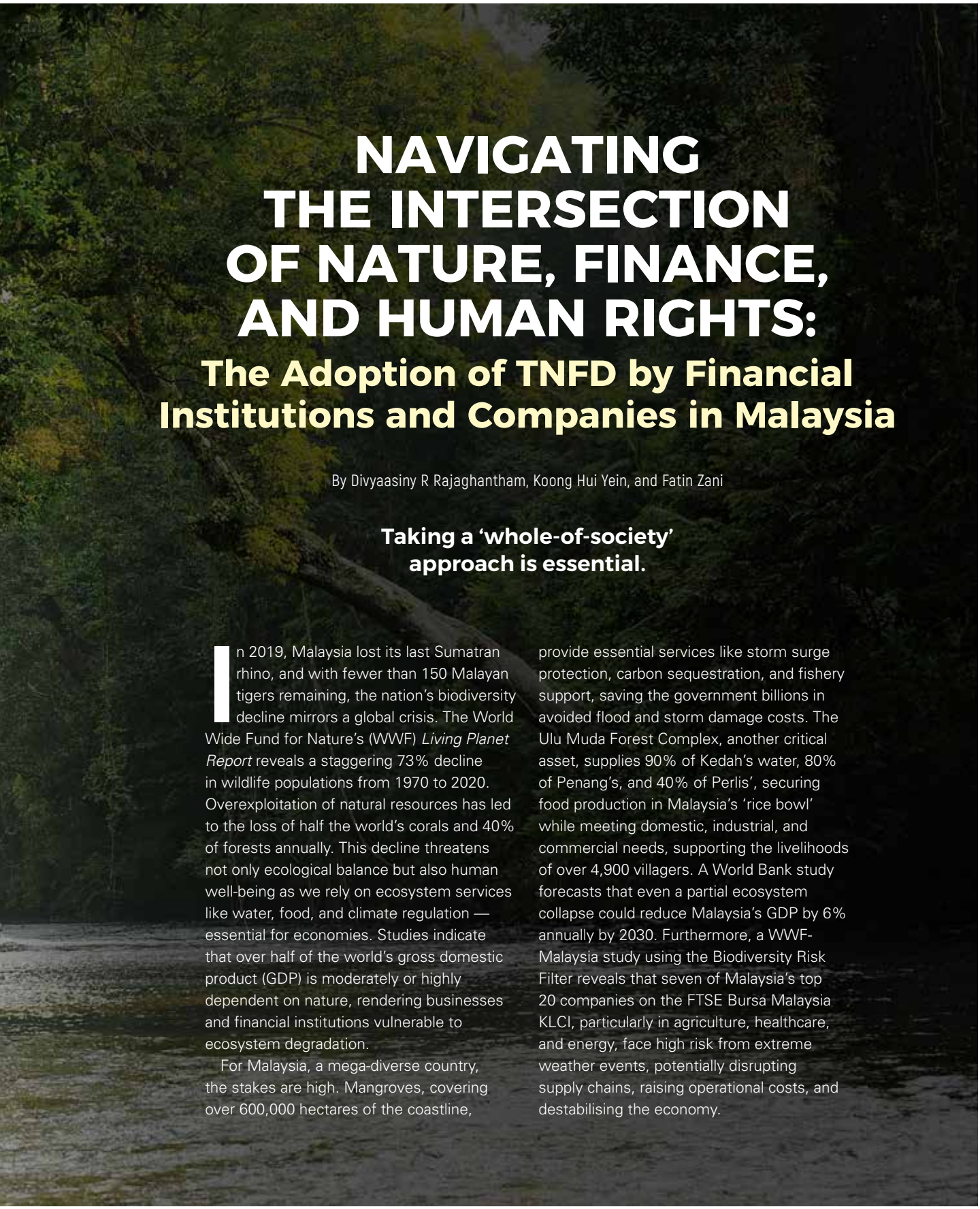
What is certain is that crypto regulation has reached a hard fork of its own – one in which a concerted resolution by regulators will be needed…and soon. Custodia's Long portends: "Bitcoin's going to take a G-SIB (global systemically important bank) down at some point because they don't understand that the settlement risk is so different between bitcoin and traditional assets."

With the increased intermingling of investments between traditional and digital asset classes, the question today isn't whether there will be a 'safe harbour' for crypto in banking, but whether banking is safe at all if crypto is not formally brought into the fold. ✱

What is certain is that crypto regulation has reached a hard fork of its own – one in which a concerted resolution by regulators will be needed…and soon. Custodia's Long portends: "Bitcoin's going to take a G-SIB (global systemically important bank) down at some point because **THEY DON'T UNDERSTAND THAT THE SETTLEMENT RISK IS SO DIFFERENT BETWEEN BITCOIN AND TRADITIONAL ASSETS.**"

■ *Angela SP Yap is a multi-award-winning social entrepreneur, author, and financial columnist. She is Director and Founder of Akasaa, a boutique content development and consulting firm. An ex-strategist with Deloitte and former corporate banker, she has also worked in international development with the UNDP and as an elected governor for Amnesty International Malaysia. Angela holds a BSc (Hons) Economics.*

■ *Kannan Agarwal is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*



NAVIGATING THE INTERSECTION OF NATURE, FINANCE, AND HUMAN RIGHTS:

The Adoption of TNFD by Financial Institutions and Companies in Malaysia

By Divyaasiny R Rajaghantham, Koong Hui Yein, and Fatin Zani

Taking a 'whole-of-society' approach is essential.

In 2019, Malaysia lost its last Sumatran rhino, and with fewer than 150 Malayan tigers remaining, the nation's biodiversity decline mirrors a global crisis. The World Wide Fund for Nature's (WWF) *Living Planet Report* reveals a staggering 73% decline in wildlife populations from 1970 to 2020. Overexploitation of natural resources has led to the loss of half the world's corals and 40% of forests annually. This decline threatens not only ecological balance but also human well-being as we rely on ecosystem services like water, food, and climate regulation — essential for economies. Studies indicate that over half of the world's gross domestic product (GDP) is moderately or highly dependent on nature, rendering businesses and financial institutions vulnerable to ecosystem degradation.

For Malaysia, a mega-diverse country, the stakes are high. Mangroves, covering over 600,000 hectares of the coastline, provide essential services like storm surge protection, carbon sequestration, and fishery support, saving the government billions in avoided flood and storm damage costs. The Ulu Muda Forest Complex, another critical asset, supplies 90% of Kedah's water, 80% of Penang's, and 40% of Perlis', securing food production in Malaysia's 'rice bowl' while meeting domestic, industrial, and commercial needs, supporting the livelihoods of over 4,900 villagers. A World Bank study forecasts that even a partial ecosystem collapse could reduce Malaysia's GDP by 6% annually by 2030. Furthermore, a WWF-Malaysia study using the Biodiversity Risk Filter reveals that seven of Malaysia's top 20 companies on the FTSE Bursa Malaysia KLCI, particularly in agriculture, healthcare, and energy, face high risk from extreme weather events, potentially disrupting supply chains, raising operational costs, and destabilising the economy.

Figure 1 Aerial view of forest next to palm clearing in Sabah, Malaysia.
Source: © Aaron Gekoski / WWF-US.

Amidst growing nature loss concerns, Malaysia has taken steps to strengthen biodiversity protection through policy direction and targeted initiatives. As one of the early adopters of the Kunming-Montreal Global Biodiversity Framework (GBF), Malaysia integrated the GBF's goals into its National Biodiversity Strategy and Action Plan, releasing the National Policy on Biological Diversity 2022–2030 last year. At the 16th session of the Conference of the Parties (COP16), Malaysia reiterated its commitment to protect biodiversity, with plans to expand protected areas, advocate for nature-based solutions, address poaching and illegal logging, and enhance monitoring practices. While ongoing, these efforts reflect the government's commitment to accountability in biodiversity efforts, aligning them with economic resilience and climate goals.

THE ROLE OF TNFD IN ADDRESSING NATURE LOSS

In parallel with government action, GBF's Target 15 calls on the private sector to assess, disclose, and manage their nature-related dependencies, impacts, and risks by 2030. The Taskforce on Nature-related Financial Disclosures (TNFD) aligns with Target 15 by providing a framework for companies and financial institutions to assess and communicate their interaction with nature. The underlying idea is that corporations are more likely to protect nature as part of their business when they understand their dependency on it. For instance, a cocoa company may choose to invest in pollinator protection once it understands the impact of declining insect populations on its crop yields.

The TNFD, a market-led, government-supported, and science-based initiative, offers a risk management and disclosure framework for the private sector to manage their nature-related issues. Over 500 organisations have committed to TNFD-aligned risk management and corporate reporting. While still in its early adoption phase, momentum is growing in Malaysia – three corporations have signed on as TNFD Adopters, committing

Figure 2 Overview of the TNFD Recommended Disclosures and its alignment with the TCFD Recommended Disclosures.
Source: *TNFD In A Box - Module 2: Overview of the TNFD.*

Figure 3 WWF Biodiversity Risk Filter alignment with TNFD LEAP approach.
Source: *WWF Tackling Biodiversity Risks,* WWF.

to prepare their nature-related disclosures by 2025. Additionally, Bank Negara Malaysia, a TNFD Forum member, is collaborating with the World Bank to develop nature-related financial risk assessment guides for the country's financial institutions and businesses.

Recognising the climate-nature nexus, the TNFD builds extensively on the work of its sister initiative, the Task Force on Climate-related Financial Disclosures (TCFD). The TNFD adopts TCFD's language and structure of governance, strategy, risk [and impact] management, and metrics and targets. The TNFD incorporates all 11 of the TCFD's recommendations, recontextualised for nature for ease of adoption. To address the unique challenges of assessing nature-related risks, the TNFD has included three additional recommended disclosures addressing supply chains and human rights in nature risk assessments and the spatial specificity of nature risks.

With the rise of environmental, social, and governance (ESG) disclosure standards, interoperability between frameworks is pivotal for private sector adoption. The TNFD recommendations are consistent with the International Sustainability Standards Board's (ISSB) International Financial Reporting Standards Sustainability Disclosure Standards, which serve as the global baseline for sustainability reporting. The ISSB has indicated its intention to incorporate nature-related corporate reporting requirements informed by TNFD's work. Given ISSB's foundational role in Malaysia's newly announced National Sustainability Reporting Framework and considering global standards like the European Union Corporate Sustainability Reporting Directive, which mandates biodiversity reporting under the European Sustainability Reporting Standards E4 requirement, trends suggest that nature reporting requirements may soon mirror those for mandatory climate reporting. While TNFD remains voluntary for now, early adoption will enable Malaysian businesses to align with global standards, facilitating their transition to mandatory disclosures.

Recognising the climate-nature nexus, the **TNFD BUILDS EXTENSIVELY ON THE WORK OF ITS SISTER INITIATIVE, THE TASK FORCE ON CLIMATE-RELATED FINANCIAL DISCLOSURES (TCFD)**. The TNFD adopts TCFD's language and structure of governance, strategy, risk [and impact] management, and metrics and targets.

Recognising the difficulties of assessing nature-related risks, TNFD also developed the LEAP framework, which guides organisations through four phases (locate, evaluate, assess, and prepare). Each phase is supported by guiding questions to help businesses evaluate their dependencies on nature, assess risks and opportunities, and integrate these insights into their strategies and disclosures. Though not compulsory, the LEAP approach complements the

TNFD framework, easing the disclosure process. Tools like Exploring Natural Capital Opportunities, Risks and Exposure (ENCORE) and WWF's Risk Filter Suiteoffer accessible entry points for companies to understand material nature-related risks based on their sector and location.

Metrics remain central for tracking progress. Unlike climate, which can be quantified by CO_2 emissions, nature encompasses complex, multidimensional factors which cannot be reduced to a single metric. The TNFD's initial survey reveals that companies are using over 3,000 metrics for their nature-related disclosures. To enhance comparability, TNFD distilled these metrics into 'core global metrics' applicable across all sectors and 'core sector metrics' tailored to specific industries, reported on a 'comply or explain' basis, with additional metrics recommended to capture material nature-related issues as needed. Given nature's unique characteristics and the growing demand for high-quality, timely, and assurable nature-related data, the TNFD announced at COP16 the release of a roadmap to improve market access to decision-useful data, which includes the development of an open-access Nature Data Public Facility in collaboration with partners like WWF.

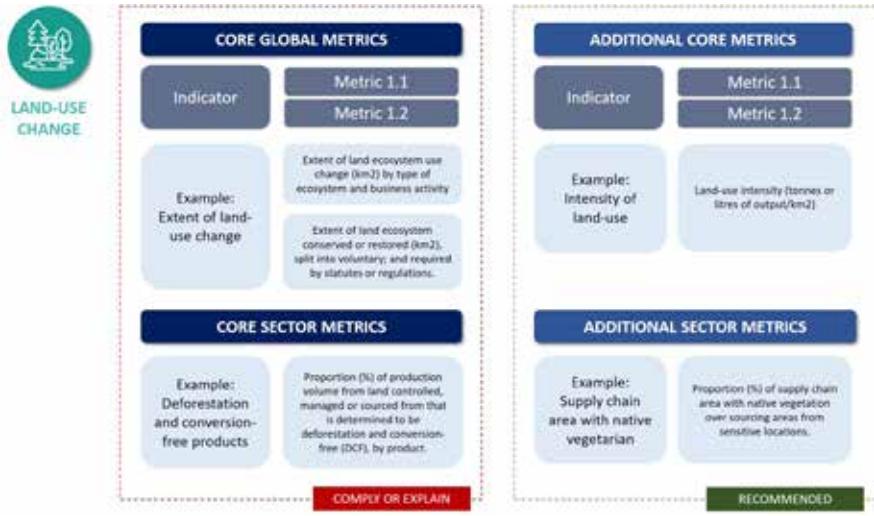


Figure 4 Example of land-use change metrics of a company from the food and agriculture sector.
Source: TNFD Recommendations - September 2023; *TNFD Additional sector guidance - Food and agriculture, TNFD.*

FPIC: BRIDGING INDIGENOUS RIGHTS AND NATURE PROTECTION

In 2018, the indigenous Semai people of Kampung Ulu Geruntum in Perak took legal action against two companies and the state government for constructing a micro-hydro dam on their traditional land without consent. This dam potentially threatened the water source for hundreds of families and endangered vital natural resources for indigenous communities. Additionally, it posed a risk to the region's ecotourism, impacting its rich biodiversity, including the Rafflesia flower, the world's largest single bloom. The September 2024 ruling by the Ipoh High Court in favour of the Semai people serves as a critical reminder for businesses – even in clean sectors like renewable energy — of the necessity to respect indigenous rights, particularly the right to free, prior, and informed consent (FPIC), as we transition towards a lower-carbon and nature-positive economy.

People are an integral part of nature. Nature loss can pose a profound social crisis, particularly affecting indigenous peoples and local communities (IPLCs) who depend on biodiversity for food, water, and livelihoods. The IPLCs safeguard 24% of global above-ground carbon and 80% of biodiversity-rich territories, making their traditional knowledge vital in combating biodiversity loss. The GBF acknowledges the significance of IPLCs, promoting an inclusive, rights-based conservation approach that emphasises FPIC. According to the United Nations Declaration on the Rights of Indigenous Peoples, the right to FPIC empowers IPLCs to negotiate terms for projects impacting their lands, thereby safeguarding their rights and cultural heritage. For businesses and financial institutions, respecting FPIC is not merely a legal obligation; it is a moral imperative, promoting sustainable and ethical practices.

Building on the GBF's principles, the TNFD emphasises the role of IPLCs in achieving sustainable, nature-positive outcomes. In addition to highlighting the role of engagement and human rights in its recommended disclosures, the TNFD released the *Guidance on Engagement with Indigenous Peoples, Local Communities, and Affected Stakeholders*. The document aims to help companies and financial institutions conduct meaningful engagements with IPLCs and affected stakeholders in nature-related risk assessments, ensuring their rights are upheld and insights are integrated into corporate decision-making. This approach mitigates risks while fostering long-term resilience for both nature and local communities.

While informative, the TNFD recognises that its guidance only addresses human rights issues related to nature, connected to an organisation's business model and value chain. Although aligned, global standards such as the United Nations Guiding Principles on Business and Human Rights offer a broader framework for business to incorporate human rights and environmental due diligence into their operations. These principles obligate companies to respect human rights across their supply chains and to avoid contributing to abuses. By adopting proactive measures to prevent harm, businesses can uphold ethical standards and enhance their long-term sustainability and reputation in an increasingly socially conscious marketplace.

THE CHALLENGES AND OPPORTUNITIES OF AN INCLUSIVE NATURE-POSITIVE BUSINESS IN MALAYSIA

According to the *2024 WWF Sustainable Banking Assessment,* only 36% of Malaysian banks have policies directing clients to obtain FPIC from affected communities and grievance mechanisms in place, suggesting a significant gap in effective implementation of FPIC within the financial sector. For businesses to remain competitive and ethical, they must balance growth with social and environmental responsibility, adhering to both local laws and international standards. Sectors like palm oil and timber face increasing scrutiny from international consumers who expect compliance with standards such as the Roundtable on Sustainable Palm Oil and the Forest Stewardship Council. These standards emphasise FPIC requirements, ensuring local communities are informed and consulted before development projects commence. However, implementation can vary widely with power imbalances, language barriers, and inadequate compensation compromising FPIC's effectiveness in protecting indigenous rights and promoting sustainable development.

Despite these challenges, integrating the FPIC principles can unlock new opportunities. The Kuamut Rainforest Conservation Project in Sabah exemplifies a successful public-private partnership that engages local indigenous communities in land use and conservation planning. Through transparent communication and meaningful dialogue, the project fosters trust and collaboration, ensuring community rights and concerns are respected. The initiative demonstrates that by honouring indigenous rights and engaging the correct partners, FPIC can be effectively integrated into project design and execution, leading to successful outcomes.

CONCLUSION

As we transition towards net-zero and nature-positive development, businesses and financial institutions must acknowledge that addressing both nature loss and human rights is vital for sustainable growth. A 'whole-of-society' approach, involving businesses, financial institutions, civil societies, and public entities, is essential. Frameworks like the TNFD and FPIC can help guide the private sector in navigating the complexities of nature, finance, and human rights, while proactively aligning with emerging trends to meet evolving ESG disclosure requirements and growing policy expectations. By safeguarding natural ecosystems and upholding indigenous rights, businesses can mitigate risks and seize new opportunities, building a future where people and nature thrive together. ✱

■ *Divyaasiny R Rajaghantham, Koong Hui Yein, and Fatin Zani are part of the Sustainable Finance team at WWF-Malaysia. Together, they support sustainable finance initiatives in collaboration with regulatory authorities, financial institutions and companies, driving the integration of ESG policies in the sector.*

Figure 5 LEAP Approach and questions for engagement.
Source: TNFD *Guidance on Engagement with Indigenous Peoples, Local Communities and Affected Stakeholders,* TNFD.

Risky Business

By Chartered Banker Institute

While the challenges that chief risk officers have to be aware of are apparent, their specific roles within their organisations are often less known. Two industry experts to shed light on current best practices.

The chief risk officer (CRO) role is by no means a well-established one. In fact, it's widely believed that James Lam became the first person to formerly hold this title at GE Capital just over 30 years ago. And since its incarnation, this position has evolved from solely monitoring risk to having the ability to veto strategic decisions. Today, to say that CROs are of the upmost importance is somewhat of an understatement. Take Silicon Valley Bank (SVB), which folded last year and had been without one for eight months prior to its shock collapse.

Laura Izurieta stepped down from her role as CRO of SVB Financial Group in April 2022, and formally left the company in October. Her permanent successor, Kim Olson, did not join until 4 January 2023, a mere matter of months before the bank failed. It is unclear how the bank managed risks between the departure of one CRO and appointment of another, and this fact formed part of the Federal Reserve's investigation into the bank's demise.

Alan Greenspan, the American economist who served as the 13th Chairman of the Federal Reserve from 1987 to 2006, went as far as to state that better risk management may be the only truly necessary element of success in banking. But what exactly does the function entail? How, for example, are emerging risks tracked and cascaded throughout the organisation?

THREE LINES

David Coleman, Vice President, CRO, European Bank for Reconstruction and Development (EBRD), initially looks to answer this question by introducing a 30-year-old concept – the three lines of defence, now known just as 'three lines'.

The first line of defence, he explains, is everyone. "All of the people in an organisation have to accept that they have a role to play in identifying, reporting, managing and mitigating risks," he says. "But because many people are given business goals linked to bonuses, that leads to a slight bias away from reporting risk.

"Then we have a second line. These are people who are not rewarded by the business for goals and objectives but are recognised for providing an objective view through an independent reporting line to the CRO."

The third and final line of defence is the internal audit function. "Here," Coleman continues, "we have a very small risk assessment team that carries out sample checks and sample audits of the second and first lines of defence to make sure they're conforming with the policies and are doing what they're meant to."

Coleman emphasises that it's vital to remember that the first line has culture and leadership at its heart. "The first line is the part we are really tackling, and this means that when managing, promoting and rewarding people, their goals and objectives should have a component of risk management.

"And this needs to extend beyond, 'I have to tell the truth', and instead it should include how a department and team are run, if rules are being followed in terms of how payments are arranged, how they record bookings and are four-eye controls being exercised? It should be all-encompassing and should feature incentives and recognition."

AN ALL-IMPORTANT PIECE OF THE JIGSAW

Greg Jones, CRO, Europe and Asia Region, TD Securities, shines a light on the structural and minimum standard policies and procedures that risk follows. "These are called risk and control self-assessments (RCSA)," he explains, "and they are the scheduled, structured frameworks and policies we follow – they are essentially the basic level that we should be working with. Think top and emerging risk reviews, reactions to operational events, assessment lessons learnt and avoidance of repetitive events.

"These are carried out to ensure that we meet standard regulatory expectations for risk identification, risk assessment and risk management, and they are growing considerably." Echoing Coleman, Jones explains that there's a definite focus on making sure that awareness and attention are key from the start of any contact with a client or a business, all the way through to second-line controls and management, through to third-line assessment and checking.

That's the extra piece [of the puzzle] that's needed with risk – considering what could potentially go wrong. The risk manager's job is to **LOOK AHEAD AND IDENTIFY WHERE THERE MIGHT BE EXPOSURE** that might not have otherwise triggered a concern within the business. The function's ability to do this depends upon the commercial awareness within the team.

"These are very much established and are the responsibilities that must be performed," Coleman emphasises. "They are the window through which a regulator looks into a bank.

"Then there's being reactive. Some banks will call this horizon scanning, and I think that's where you get the true value." Jones stresses that in order to succeed here, firms have to have a risk management function that has the capacity, resources, skills and the commercial awareness to look at what is coming ahead – as well as the ability to discuss it with the business.

"The business might tell you that they want to be big in a certain client sector – for example chip manufacturing," says Jones.

"And the risk function might come back and say, "That's great, but have you considered that this particular chip manufacturer is in the tornado zone in the US?". You might also have to point out that the weather is getting worse, which means they'll face physical environmental, social, and governance risks.

"That's the extra piece [of the puzzle] that's needed with risk – considering what could potentially go wrong. The risk manager's job is to look ahead and identify where there might be exposure that might

not have otherwise triggered a concern within the business. The function's ability to do this depends upon the commercial awareness within the team.

"Risk needs to be close to the business and challenging the business. Discussions should be taking place at a commercial level, too. It's not just about performing the regulator-required tasks."

CONSEQUENCES, RESILIENCE AND FIELDING THREATS

Coleman, meanwhile, believes that a key aspect of effective risk management is ensuring that that the CRO and the risk team do not become excessively focused on the running of the organisation.

"The inward-looking issues should not be their main focus," he advises. "Instead, they should have the time, the space and the resource to be looking outwards, networking, intelligence-gathering and future-gazing. This role isn't about excessive brainstorming, it's about thinking about the consequences of certain events, and whether the company is prepared.

"Members of the risk team should ask themselves if the firm is prepared for a change of US government, or a change of the national government where the firm is based. Is the firm prepared for the new regulations or for the impact that a war could have on food and energy and inflation?"

The inward-looking issues should not be their main focus," he advises. "Instead, they should have the time, the space and the resource to be looking outwards, networking, intelligence-gathering and future-gazing. **THIS ROLE ISN'T ABOUT EXCESSIVE BRAINSTORMING, IT'S ABOUT THINKING ABOUT THE CONSEQUENCES OF CERTAIN EVENTS,** and whether the company is prepared.

Coleman states that the CRO role also has much to do with the resilience of an organisation. "We used to have an office building in central London, in the City," he recalls. "And that building was of vital importance. We had all of our services and provision of support in that building, including two-thirds of our workforce and a data centre. "Clearly, we can look back and say that that was not a particularly resilient business model. Nor was it necessarily the most effective, given the fact that many others had already started outsourcing."

Today, the EBRD has a more complicated business model. "We have a significant reliance on external suppliers for services, including some of them around IT," explains Coleman. "Our data centre is no longer part of the main building, which is a good idea.

"We've also placed some of our support services into our branch network rather than having them in our headquarters. This makes it more efficient but it does mean complications in our business model. We've been through a pandemic where we had to learn to operate the entire business model from home, which was something we'd never conceived of prior to Covid."

What this means, he explains, is that business resilience has taken on a whole new level of complexity. "And although some of the challenges that we went through, including outsourcing and offshoring and having separate data centres, are factors that other companies had been dealing with for many, many years, we all still had to learn how to deal with a pandemic.

"Some people will have regretted where or to whom they outsourced because the world has changed and continues to do so. And just because a firm has outsourced to a major supplier, it doesn't mean that they will be there every day. These are internal threats, but businesses still need to think about them."

EYES ON THE HORIZON

How can businesses ensure that early identification is a priority within the risk function? According to Jones, this starts

with the inherent threats that encircle the business. "What controls do we have against those inherent risks? And then, how are those controls performing? What's emerging and what might need additional controls? That's a formulaic piece.

"We have business economists and strategists," he continues. "They're looking forward. They're looking at what's on the horizon, what's going to affect their portfolios and what their decision is going to be for forthcoming business objectives. But what's needed is getting that feedback loop into your risk assessment process."

Capturing and quantifying the risk, he says, is of the utmost importance. "Every bank faces operational risks in terms of resilience, tech platforms and modernisation. Is your company, for example, missing updates? Truth be told, even the biggest banks with the largest budgets probably struggle to keep a resource pool sufficient to continually evolve."

Banks, he believes, operate best when they push the right level of authority down through the business. "If we suck all authority up to the top, then the processes aren't efficient. We need – throughout the business – commercial awareness, knowledge, competence, and confidence. And confidence leads to independence, which in turn leads to good control.

"Then those foundation blocks of confidence and independence control enable more authority to be pushed out, and more discretion to move lower down into the organisation. All of this means more effective and more timely responses to the business. This should also ensure that information flows up."

Ultimately, this means that if the right blend of capabilities doesn't exist on the lower levels, more processes fall to the mid and high levels, which therefore have to be higher touch. "If this happens," says Jones, "there will be senior people looking at granular data when they shouldn't be. Instead, they should be looking at the core consideration operations around the business.

"The lower tiers should be the confident, independent and informed controllers 'at the bottom', and they should know what information needs to go up."

We have to promote networking. **WE SHOULDN'T ASSUME THAT OUR BANK IS DOING EVERYTHING IN THE BEST POSSIBLE WAY.** The chances are it isn't. We also have to push our risk controllers to get a flavour for risk management across the whole market. And you become aware of market standards by networking – by sharing with peers and other banks.

PLACING THE LAST PIECE OF THE PUZZLE

"We have access to the business, commercial awareness and access to management – and that leaves one missing piece of the puzzle, which is networking," says Jones.

"We have to promote networking. We shouldn't assume that our bank is doing everything in the best possible way. The chances are it isn't. We also have to push our risk controllers to get a flavour for risk management across the whole market. And you become aware of market standards by networking – by sharing with peers and other banks. You don't have to try to have facetime with J.P Morgan. There are other banks that have been through the mill with the US regulators."

Coleman agrees: "For the risk team to function at its best, time and effort must be devoted to networking. It is vital to have people whose job it is to spend some of their time looking at what others are doing and reflecting on that. They must also think about what's coming in terms of law, regulation and market developments. They should be looking at what's happening with clients, from a climate perspective and from a technology perspective – from all perspectives, in fact. Because these factors will change your business model and the business model of your clients."

Jones concludes: "Some of what your peers do will be world-class and ahead of the game because the regulator will have pushed them to reach that standard. But you don't just have to talk to the Premiership – there's plenty that can be gleaned from the Championship and the lower divisions as well." ✱

■ *This article previously appeared in Issue 2 2024 of Chartered Banker, UK.*

Awarded by:

CHARTERED BODY ALLIANCE

Chartered Insurance Institute

CISI CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT

Chartered Banker

AICB

ASIAN INSTITUTE OF CHARTERED BANKERS

CERTIFICATE IN CLIMATE RISK

Demonstrate your knowledge and expertise in climate risk

The Certificate in Climate Risk (CICR) encompasses the study of a wide range of developments in climate change and its risks and impacts, the evolving policy and regulatory landscape, and the substantial progress in addressing climate and broader sustainability risks in the financial sector. Ideal for current or aspiring financial services professionals globally, the CICR develops your knowledge, understanding and skills on climate change, climate risk and sustainable finance, enabling you to better support your professional communities in the transition to a sustainable, low-carbon world.

To enrol, please visit www.aicb.org.my

Asian Institute of Chartered Bankers 197701004872 (35880-P) Levels 11 & 12, Bangunan AICB, 10 Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
T (603) 2602 6833 **E** enquiries@aicb.org.my

Banking Transformation in Southeast Asia: Insights from Banking Leaders

By Sash Mukherjee

Bringing down barriers to fulfill industry's tech promise.

Southeast Asia's banking sector is poised for significant digital transformation. With projected net interest income reaching USD148 billion by 2024, the market is ripe for continued growth. While traditional banks still hold a dominant position, digital players are making significant inroads. To thrive in this evolving landscape, financial institutions must adapt to rising customer expectations, stringent regulations, and the imperative for resilience. This will require a seamless collaboration between technology and business teams.

To uncover how banks in Southeast Asia are navigating this complex landscape and what it takes to succeed, Ecosystm engaged in in-depth conversations with senior banking executives and technology leaders as part of our research initiatives. Here are the highlights of the discussions with leaders across the region.

ACHIEVING HYPER-PERSONALISATION THROUGH ARTIFICIAL INTELLIGENCE (AI)

As banks strive to deliver highly personalised financial services, AI-driven models are becoming increasingly essential. These models analyse customer behaviour to anticipate needs, predict future behaviour, and offer relevant services at the right time. AI-powered tools like chatbots and virtual assistants further enhance real-time customer support. Ecosystm research finds that 74% of banks in Southeast Asia view enhancing customer experience and improving back-end processes as the key outcomes of AI adoption.

Hyper-personalisation, while promising, comes with its challenges – particularly around data privacy and security. To deliver deeply tailored services, banks must collect extensive customer information, which raises the question: how can they ensure this sensitive data remains protected? A head of customer experience at one bank explains their approach. "Most of our AI efforts focus on improving customer experience through internal applications designed for employees. But we do have one customer-facing generative AI (GenAI) app. The key here is that it's entirely disconnected from our databases. It generates a customer score by analysing responses and basic demographics, which helps us boost engagement without compromising data security."

AI projects require a delicate balance between innovation and regulatory compliance. Regulations often serve as the right set of guardrails within which banks can innovate. However, banks – especially those with cross-border operations – must establish internal guidelines that consider the regulatory landscape of multiple jurisdictions.

BEYOND AI: OTHER EMERGING TECHNOLOGIES

AI isn't the only emerging technology reshaping Southeast Asian banking. Banks are increasingly adopting technologies like robotic process automation (RPA) and blockchain to boost efficiency and engagement. RPA is automating repetitive tasks, such as data entry and compliance checks, freeing up staff for higher-value work. CIMB Bank in Malaysia reports seeing a 35%–50% productivity increase, thanks to RPA. Blockchain is being explored for secure, transparent transactions, especially cross-border payments. The Asian Development Bank successfully trialled blockchain for faster, safer bond settlements. While augmented reality and

virtual reality are still emerging in banking, they offer the potential for enhanced customer engagement. Banks are experimenting with immersive experiences like virtual branch visits and interactive financial education tools.

The convergence of these emerging technologies will drive innovation and meet the rising demand for seamless, secure, and personalised banking services in the digital age. This is particularly true for banks that have the foresight to future-proof their tech foundation as part of their ongoing modernisation efforts. Emerging technologies offer exciting opportunities to enhance customer engagement, but they shouldn't be used merely as marketing gimmicks. The focus must be on delivering tangible benefits that improve customer outcomes. As the chief innovation officer at a Philippine bank put it, "Consumers don't care about the underlying technology. They're not interested in whether we use crypto or something else – they just want seamless payments and transactions."

GREATER BANKING-FINTECH COLLABORATION

The digital payments landscape in Southeast Asia is experiencing rapid growth, with a projected 10% increase between 2024 and 2028. Digital wallets and contactless payments are becoming the norm and platforms like GrabPay, GoPay, and ShopeePay are dominating the market. These platforms not only offer convenience but also enhance financial inclusion by reaching underbanked populations in remote areas.

The rise of digital payments has significantly impacted traditional banks. To remain relevant in this increasingly cashless society, banks are collaborating with fintech companies to integrate digital payment solutions into their services. For instance, Indonesia's Bank Mandiri collaborated with digital credit services provider Kredivo to provide customers with access to affordable and convenient credit options.

Partnerships between traditional banks and fintech are essential to staying competitive in the digital age, especially in areas like digital payments, data analytics, and customer experience. "We've seen digital-native businesses achieve in 24 hours what traditional players take over six months to do," says the chief transformation officer of a bank in Malaysia. "To compete, we must collaborate with innovators."

The rise of digital payments has significantly impacted traditional banks. To remain relevant in this **INCREASINGLY CASHLESS SOCIETY**, banks are collaborating with fintech companies to integrate digital payment solutions into their services.

While these collaborations offer opportunities, they also pose challenges. Banks must invest in advanced fraud detection, AI monitoring, and robust authentication to secure digital payments. Once banks adopt a mindset of collaboration with innovators, they can leverage numerous innovations in the cybersecurity space to address these challenges.

AGILE INFRASTRUCTURE FOR AN AGILE BUSINESS

While the banking industry is considered a pioneer in implementing digital technologies, its approach to cloud has been more cautious. While interest remained high, balancing security and regulatory concerns with cloud agility impacted the pace. Hybrid multi-cloud environments have accelerated banking cloud adoption. Ecosystm research finds that 64% of banks in Southeast Asia have adopted a hybrid, multi-cloud environment – and 45% will invest more in hybrid cloud management tools in 2025.

Leveraging public and private clouds optimises IT costs, offering flexibility and scalability for changing business needs. A hybrid cloud allows resource adjustments for peak demand or cost reductions during off-peak. Access to cloud-

native services accelerates innovation, enabling rapid application development and improved competitiveness. As the industry adopts GenAI, it requires an infrastructure capable of handling vast data, massive computing power, advanced security, and rapid scalability – all strengths of the hybrid cloud.

Replicating critical applications and data across multiple locations ensures disaster recovery and business continuity. A multi-cloud strategy also helps avoid vendor lock-in, diversifies cloud providers, and reduces exposure to outages. "You don't want to be tied to one cloud. If it goes down, you need the flexibility to pivot. Spread your eggs across multiple clouds," advises the chief information officer of a bank in Thailand.

Hybrid cloud adoption offers benefits but also presents challenges for banks. Managing the environment is complex, needing coordination across platforms and skilled personnel. Ensuring data security and compliance across on-premises and public cloud infrastructure is demanding and requires robust measures. Network latency and performance issues can arise, making careful design and optimisation crucial. Integrating on-premises systems with public cloud services is time-consuming and needs investment in tools and expertise.

CYBER MEASURES TO PROMOTE CUSTOMER & STAKEHOLDER TRUST

The banking sector is undergoing rapid AI-driven digital transformation, focusing on areas like digital customer experiences, fraud detection, and risk assessment. However, this shift also increases cybersecurity risks, with the majority of banking technology leaders anticipating inevitable data breaches and outages. According to our research, 67% of technology leaders in Southeast Asia's banking sector feel that a data breach is inevitable while 58% perceive a limited understanding of governance and cyber risk management requirements among leadership. Key challenges include expanding technology use, such as cloud adoption and AI integration, and employee-related vulnerabilities like phishing. Banks in Southeast Asia are investing heavily in modernising infrastructure, software, and cybersecurity.

Banks must update cybersecurity strategies to detect threats early, minimise damage, and prevent lateral movement within networks. "In cybersecurity, the biggest challenge is that while data processing usually works as expected, rare exceptions can have catastrophic consequences, especially in sensitive industries like banking," explains the chief information security officer of a large global bank headquartered in Singapore. Employee training, clear security policies, and a culture of security consciousness are critical in preventing breaches.

Regulatory compliance remains a significant concern but banks are encouraged to move beyond compliance checklists and adopt risk-based, intelligence-led strategies. AI will play a key role in automating compliance and enhancing security operations centres, allowing for faster threat detection and response. Ultimately, the banking, financial services, and insurance sector must prioritise cybersecurity continuously based on risk, rather than solely on regulatory demands.

BREAKING DOWN BARRIERS: THE ROLE OF COLLABORATION IN BANKING TRANSFORMATION

A successful banking transformation hinges on a seamless collaboration between technology and business teams. By aligning strategies, fostering open communication, and encouraging cross-functional cooperation, banks can effectively leverage emerging technologies to drive innovation, enhance customer experience, and improve efficiency.

A prime example of the power of collaboration is the success of AI initiatives in addressing specific business challenges. As the chief data officer of a global bank with regional headquarters in Singapore noted, "One of our biggest AI successes came when customer experience employees identified their biggest problems, collaborated with the data science team, and refined the solutions." This user-centric approach ensures that technology addresses real business needs.

By fostering a culture of collaboration, banks can promote continuous learning, idea sharing, and innovation, ultimately driving successful transformation and long-term growth in the competitive digital landscape. ✱

■ *Sash Mukherjee is the Vice President of Industry Insights at Ecosystm.*

CHECK POINT: ASEAN TAXONOMY VERSION 3

By Julia Chong

FINE-TUNE UNDERWAY.

On 27 March 2024, the Association of Southeast Asian Nations' (ASEAN) Taxonomy Board (ATB) announced the most recent iteration, Version 3, of the ASEAN Taxonomy for Sustainable Finance (ASEAN Taxonomy). In line with its predecessors, Version 3 of the ASEAN Taxonomy is currently undergoing a stakeholder consultation process in order to help fine-tune the framework.

The ATB is a collaborative initiative comprising four sectoral bodies which jointly oversee the development of the umbrella framework:

- ASEAN Capital Markets Forum;
- ASEAN Insurance Regulators Meeting;
- ASEAN Senior Level Committee on Financial Integration; and
- ASEAN Working Committee on Capital Market Development.

The ATB's mandate in this regard is to introduce a common language under which sustainable economic financing can flourish and support the goals of the 26th United Nations Climate Change Conference of the Parties or COP26. At the meeting, each ASEAN member state outlined its revised nationally determined contributions (NDCs). The NDC is a national-level plan which a country submits detailing how they will reduce emissions and limit global warming. The current NDCs of ASEAN member states are summarised in **Figure 1**.

An Evaluation of ASEAN Renewable Energy Path to Carbon Neutrality, a 2023 research paper principally written by Khairul Eahsun Fahmi, PhD researcher at the University of Brunei Darussalam, gauged the status of the NDCs by ASEAN member states at the time of its writing:

"The COP26 in Glasgow in late 2021 demanded considerable efforts from governments all over the world. The meeting's key deliverables were the revised Nationally Determined Contributions (NDCs), signatories to the Glasgow Climate Pact, and the Global Coal to Clean Power Statement, which could be essential to fulfilling climate targets. The countries' long-term strategies are intended to outline tangible activities that will strengthen the desire to go beyond the NDC targets.

"Five ASEAN member states submitted updated NDCs before the COP26 meeting in 2020, while the remainder did so in 2021. In the most recent report, nine ASEAN member states established unconditional targets for lowering emissions. Only Cambodia has a conditional goal. All ASEAN member states selected the energy and agricultural industries as the main sources of the emissions reduction target when it came to sector coverage.

"Additionally, all ASEAN member states, with the exception of Myanmar, listed trash and industrial processes and product usage as additional culprits. Only the Philippines and Thailand did not classify land use, land-use change, and forestry emissions' reduction factors. In addition to conditionality and sectoral coverage, the NDCs establish a detailed range of greenhouse gas (GHG) emissions. The majority of GHGs, such as carbon dioxide (CO_2), methane (CH_4), nitrous oxide (N_2O), hydrofluorocarbons, perfluorocarbons, sulphur hexafluoride, and nitrogen trifluoride, have been included in both Malaysia and Singapore's NDCs. However, Myanmar's NDC only mentions CO_2. Aside from CO_2, which was included in all of the ASEAN member states' NDCs, nine recorded CH_4, and N_2O."

The COP26 in Glasgow in late 2021 demanded considerable efforts from governments all over the world. The meeting's key deliverables were the revised Nationally Determined Contributions (NDCs), signatories to the Glasgow Climate Pact, and the Global Coal to Clean Power Statement, which could be **ESSENTIAL TO FULFILLING CLIMATE TARGETS.** The countries' long-term strategies are intended to outline tangible activities that will strengthen the desire to go beyond the NDC targets.

A LIVING DOCUMENT

Version 1 of the ASEAN Taxonomy was released by the ATB in November 2021. The inaugural document provided a framework to kick start the discussions between private sector stakeholders and national authorities for its development. Together with the consultation which ensued, it introduced the tenets that would guide the Southeast Asian union's trajectory towards COP26's net-zero aspirations and serves as the reference point to "guide capital and funding towards activities that can help promote the systemic transformation needed for the region."

The unique feature of the ASEAN Taxonomy is its focus on harmonisation, as opposed to standardisation, of

Country	Net Zero Target	NDC Targets	Sectoral Targets
 **Brunei Darussalam**	2050	**UNCONDITIONAL** Reduce by 20% compared to business-as-usual (BAU) **CONDITIONAL** N/A	Energy: to reduce total energy consumption by 63% by 2035 compared to a BAU scenario, and to increase the share of renewables so that 10% of the total power generation is sourced from renewable energy by 2035. Land transport: to reduce carbon dioxide emissions from morning peak hour vehicle use by 40% by 2035 compared to a BAU scenario. Forestry: to increase the total gazetted forest reserves to 55% of the total land area, compared to the current levels of 41%.
 **Cambodia**	2050	**UNCONDITIONAL** N/A **CONDITIONAL** Reduce by 41.7% compared to BAU in 2030	Compared to BAU scenario in 2030 projection for GHG emissions: • Forestry and other land use (FOLU): 50% reduction; • Energy: 40% reduction; • Agriculture: 23% reduction; • Industry 42% reduction; and • Waste: 18% reduction.
 **Indonesia***	2060 or sooner	**UNCONDITIONAL** Reduce by 31.89% compared to BAU in 2030 **CONDITIONAL** Reduce by 43.20% compared to BAU in 2030	Compared to BAU scenario in 2030 projection for GHG emissions: • FOLU: 25.4% reduction; • Energy: 15.5% reduction; • Agriculture: 0.4% reduction; • Industrial processes and product use: 0.3% reduction; and • Waste: 1.5% reduction.
 **Lao People's Democratic Republic**	2050 or sooner	**UNCONDITIONAL** Reduce by 60% compared to BAU in 2030 **CONDITIONAL** N/A	Compared to BAU scenario in 2030: • Land use, land-use change and forestry (LULUCF): Reduce by 45,000 $ktCO_2e$/year to increase forest cover to 70% of land area; • Final energy consumption: Reduce by 280 $ktCO_2e$/year, i.e. 10% reduction; • Agriculture: 128 $ktCO_2e$/year with 50,000 hectares adjusted water management practices in lowland rice cultivation; and • Waste: 40 $ktCO_2e$/year through implementation of 500 tonnes/day sustainable municipal solid waste.
 **Malaysia**	2050	**UNCONDITIONAL** Reduce by 45% of carbon intensity against GDP 2030 **CONDITIONAL** Reduce by 45% emission intensity from 2005 levels	No breakdown of sectoral targets but mentions of sectors, gases, categories, and pools covered by NDCs. Key sectors are energy, industrial processes and product use, waste, agriculture, LULUCF.
 **Myanmar**	2040 for FOLU	**UNCONDITIONAL** Reduce to 244.52 million tCO_2e by 2030 **CONDITIONAL** Reduce to 414.75 million tCO_2e by 2030 with international finance and support	Energy sector: Increase renewable energy technology to 53.5% from BAU by 2030. Agriculture: Achieve 10.4 million tCO_2e/year cumulative GHG sequestration in 2021–2030. FOLU: Reduction of 50%/year of net emission by 2030.
 **Philippines**	N/A	**UNCONDITIONAL** Reduce 2.71% compared to BAU in 2030 **CONDITIONAL** Reduce 72.29% compared to BAU in 2030	Does not provide a breakdown of their sectoral targets but divide actions into two categories: climate change mitigation and climate change adaptation.

Country	Net Zero Target	NDC Targets	Sectoral Targets
Singapore	2050	**UNCONDITIONAL** Reduce to 60 million tCO_2e emission level by 2030 **CONDITIONAL** N/A	No breakdown of sectoral targets but mentions of sectors, gases, categories, and pools covered by NDCs. Key sectors are energy, industrial processes and product use, agriculture, LULUCF, waste.
Thailand	2065 (carbon neutrality target by 2050)	**UNCONDITIONAL** Reduce 45% compared to BAU in 2030 with international finance and support **CONDITIONAL** Reduce 25% compared to BAU in 2030	Reduction in GHG emissions: • Energy: 67.2%–71.65%; • Industry: 8.61%–8.90%; • Agriculture: 19.93%–14.72%; and • Waste: 4.26%–4.73%.
Vietnam	2050	**UNCONDITIONAL** Reduce 15.8% compared to BAU in 2030 **CONDITIONAL** Reduce 43.5% compared to BAU in 2030	Reduction in GHG emissions compared to BAU scenario: • LULUCF: 5.4%; • Energy: 24.4%; • Agriculture: 5.5%; • Industry: 5.4%; and • Waste: 3.2%

Figure 1 Summary of ASEAN member states' NDCs
** The latest Indonesian NDC submitted in August 2024 states that Indonesia will adopt the 2019 reference point as mandated by COP decisions instead of the current 2030 BAU scenario, which will be integral to the formulation of the country's second NDC. It will also commit to achieving negative emissions by 2060 based on comparisons with 2019 emission levels.*

sustainable frameworks throughout the diverse region. Many are still heavily dependent on fossil fuels with each of the 10 member states (with an 11th member state, Timor-Leste, currently under discussion for inclusion) at various stages of economic development, making the transition to a low-carbon future more challenging.

From the outset of its initial 87-page document, the ASEAN Taxonomy maps the different possible transition paths for service-based economies such as Malaysia and Singapore versus the oil-and-gas-dependent nations of Brunei Darussalam and Indonesia. This is reflected in the taxonomy's principles-based approach which is built upon two tiers: a Foundation Framework (FF) whereby an economic activity must fulfil certain criteria and is classified based on a colour-coded system of green, amber, or red; and a Plus Standard (PS) which further screens an activity through application of the technical screening criteria (TSC) to more accurately determine its place in the taxonomy. The PS is also intended to facilitate inclusivity among member states, allowing for different levels of adoption depending on each country's individual readiness.

Many are still heavily dependent on fossil fuels with each of the 10 member states (with an 11th member state, Timor-Leste, currently under discussion for inclusion) at various stages of economic development, **MAKING THE TRANSITION TO A LOW-CARBON FUTURE** more challenging.

This approach stands in stark contrast to the pathway adopted by other unified groupings, such as the European Union, which are essentially binary, i.e. a business activity is classified as either 'green' or 'brown' – an approach that does not fully account for transition activities where low-carbon alternatives are not yet fully realisable.

In March 2023, the ATB released Version 2 which included the TSC for the electricity, gas, steam, and air conditioning supply (energy) sector, providing specific guidance on how it should be applied. Version 2 became effective on 19 February 2024 after incorporating feedback from stakeholder consultations.

In its latest iteration on 27 March 2024, the ASEAN Taxonomy Version 3 made public the TSC for two more focus sectors: transportation and storage (e.g. urban and freight transport, and infrastructure for land, water, and air transport) and construction and real estate (e.g. construction and renovation of buildings, demolition and site preparation, and acquisition and ownership of buildings).

Other refinements are:

- additional clarification and worked examples for the Life Cycle Assessment checklist per Annex 2;
- additional clarification and worked examples for the Climate Risk and Vulnerability Assessment checklist per Annex 3;
- updated national social regulations for Indonesia, Malaysia, and the Philippines per Annex 5; and
- updated national environmental regulations for Indonesia and Malaysia per Annex 6.

The incorporation of stakeholder feedback and lessons learnt from on-the-ground rollouts in member states from previous consultation rounds means that the focus has also increased in other key areas, including interoperability with the EU Taxonomy and other national taxonomies. Interoperability means that there is, at the macro level, a symbiotic relationship between the development of these different yet similar taxonomies. For instance, Version 3 notes that national taxonomies in ASEAN "vary in scope and approaches based on the different priorities, tolerances, and pathways in their own respective jurisdictions, but all also need to reflect the expectations of international investors" and illustrates this through the experience of Malaysia and other Southeast Asian nations.

"Bank Negara Malaysia's *Climate Change and Principle-based Taxonomy* utilises a principles-based approach and considers the state of economic development of the country and their nascent stage of climate risk management at which businesses and other economic agents operate. Although this Taxonomy mainly aims to address climate change, there are some biodiversity considerations that are also integrated within the Guiding Principles. Malaysia's capital market regulator, the Securities Commission Malaysia, also developed the Sustainable and Responsible Investment Taxonomy, to enable capital market participants to identify economic activities that are aligned with the environment, social, and sustainability objectives. The intention of this is to facilitate a more informed and efficient decision-making process for fundraising and investing."

REGIONAL POISE

The ASEAN Taxonomy has drawn on learnings from the EU Taxonomy and intends to be interoperable with it as well as other international and national taxonomies. What needs to be emphasised is the symbiotic and consultative nature embedded in the development of these taxonomies, which at the end of the day must all be geared towards achieving climate targets and increased global sustainability.

As momentum builds within ASEAN to reinforce the global net-zero climate goals by 2050, a multitude of other initiatives have sprouted to support this at various levels throughout the Asia-Pacific region. It is indication that the region itself is poised to be a vibrant and supportive ally in the quest for climate justice in finance. Such diverse views should feature considerably in how ASEAN intends to refine its approach in one that is as unique as its individual member states. ✱

■ *Julia Chong is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*

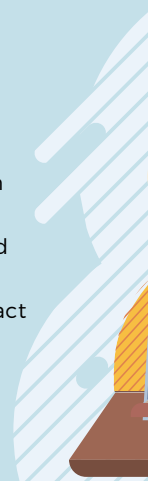
ASEAN TAXONOMY PRIMER

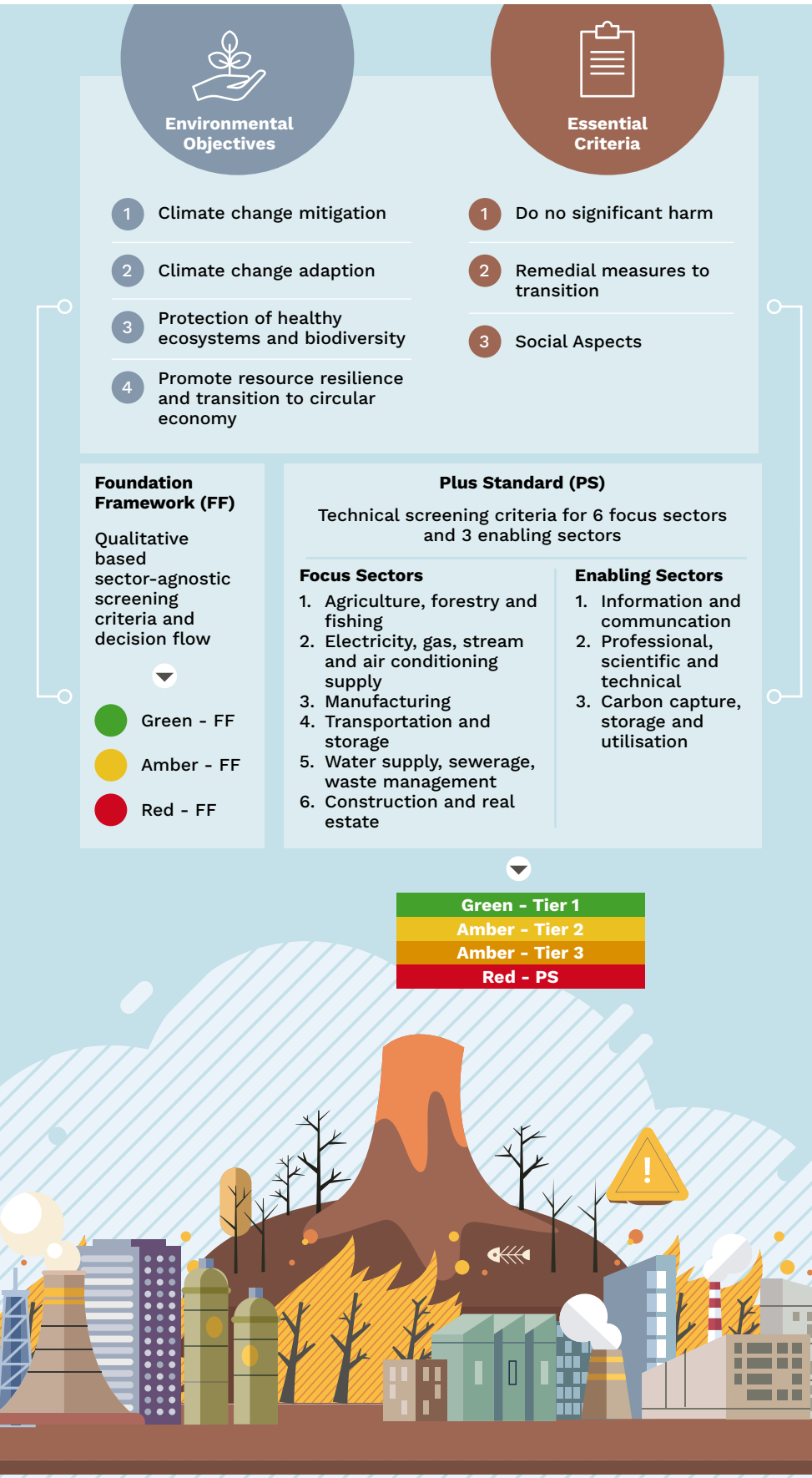
The Foundation Framework (FF) comprises four environmental objectives and three essential criteria. The four environmental objectives to which an economic activity must contribute are:

- climate change mitigation;
- climate change adaptation;
- protection of healthy ecosystems and biodiversity; and
- promote resource resilience and transition to a circular economy.

The three essential criteria also require that an activity does not violate the following rules:

- **Do no significant harm:** A pre-emptive principle which focuses on avoiding negative impact to the climate and environment.
- **Remedial measures to transition:** Ensuring an economic activity can transition to a low-carbon economy without causing disruptive exclusions or dislocations. This considers companies that are taking credible and immediate remedial actions as transitioning although currently engaged in environmentally harmful activities.
- **Social aspects:** Includes consideration of three key social aspects – promotion and protection of human rights, prevention of forced labour and protection of children's rights, and impact on people living close to investments.





The Plus Standard (PS) assessment approach robustly defines the technical screening criteria or TSC required to classify an economic activity using both threshold-based and practice-based metrics. The PS also identifies six focus sectors and three enabling sectors which are particularly important to the ASEAN sustainability journey given their significant contributions to both GHG emissions and the economy of Southeast Asia.

Both the FF and PS assessment approaches use a colour-coded classification system to represent the different levels of contribution to an environmental objective:

GREEN
An activity is making a substantial contribution.

AMBER
While not meeting the 'green' classification criteria, there is progressive movement on the path to a more sustainable ASEAN with due consideration to the practicalities of implementing sustainable activities. For the PS approach, there are two tiers to 'amber' which serves as a transition category and stepping stone for entities to make adjustments with the ultimate goal of reaching the 'green' tier. This allows for a more granular and accommodating approach which takes into account the different levels of development of each member state.

RED
An economic activity is not aligned and/or causes significant harm.

Figure 2 Structure of the ASEAN Taxonomy
Source: *ASEAN Taxonomy for Sustainable Finance*, ATB, 25 April 2024.

NUDGING ALONG: HOW BEHAVIOURAL ECONOMICS INSPIRES PRODUCT, PRICING & LOYALTY

By Kannan Agarwal

In an increasingly competitive landscape, a different lens brings fresh perspective.

Are humans rational? Through the lens of behavioural economics, the answer is clearly 'no'.

In a recent Banking Transformed podcast, Melina Palmer, CEO of The Brainy Business and author of *The Truth About Pricing: How to Apply Behavioral Economics so Customers Buy,* explains:

"The first and most important thing for everyone to know is to understand how our brains really work because that shows how important it is to be considering psychology. When we look at the way we make decisions, we like to think that the supercomputer in our head is very logical and going by the book for everything all the time and making rational choices about absolutely everything and that we're in full control of any decisions that we are making.

"In reality, the subconscious is actually making the bulk of decisions that we have at any given time and it's using rules of thumb, it's using predictability, it's using habits to make those decisions. Research has shown that each person makes 35,000 decisions a day on average. When we put it in that context, we realise how many decisions we're actually making. I love to ask people, 'How many decisions do you remember making yesterday?'"

The reason why we do not register the bulk of our decisions is because much of our decision-making is done at the subconscious level. "The rules that the brain is using to make decisions," says Palmer, "is the field of behavioural economics and in behavioural science."

EMPIRICAL THOUGHT

For many, behavioural economics is currently basking in the sun. Psychologist and Nobel Laureate the late Dr Daniel Kahneman, one of the founding fathers

of behavioural economics, upended the premise of rational decision-making in modern economics by proving how neurological human biases lead to irrational decisions. Here are some examples which make up the body of work he jointly developed with Amos Tversky:

- **Prospect theory:** Most people would drive an extra 10 minutes to save $10 on a $50 toy, however, they will not drive 10 minutes to save $20 on a $20,000 car. The gain from driving the extra 10 minutes for the car is twice the gain of driving the extra 10 minutes for the toy. Logically, more people should drive the longer distance for the double saving on the car but do not because their decision-making relies on the framing of the conundrum. Instead of comparing the absolute saving in terms of price savings, people compare the percentage saving, which in the case of the car is very small.
- **Loss aversion:** Losses loom larger than gains. People's attitudes toward risks concerning gains differ from their attitudes when it comes to losses, e.g. people are more upset over the loss of a $10 bill compared to the joy they experience if they find one. This has influenced fields as diverse as political science and election strategies.
- **Sunk-cost fallacy:** Sunk costs – whether in terms of time, finances, or hard work – keeps us invested, or investing, in something even when it proves to be futile. Kahneman reasons that this bias "keeps people for too long in poor jobs, unhappy marriages, and unpromising research projects."
- **Frequent exposure or mere-exposure effect:** Information is not proportionately distributed; the more exposed we are to a specific piece of information, the more likely we think the same is going to occur. As Kahneman put it, "A reliable way to make people believe in falsehoods is frequent repetition because familiarity is not easily distinguished from truth." Such imperfect assumptions cause many people to misjudge and make incorrect decisions; the solution requires us to think slowly and determine whether or not the option we opt for is truly the best…or just the one we are frequently exposed to.
- **False confidence in predictions:** Kahneman himself succumbed to this early in his career. When asked to observe eight candidates' physical performance in order to predict leadership potential of a group of army privates, the team of psychologists, including Kahneman himself, confidently identified those who performed (in their estimation) the best, only to learn much later that their assessment didn't reflect how these soldiers performed during the actual officers' training. This inconsistency, however, did not register as a failure with any of the psychologists, who continued to hold steadfast to their judgments and continued to fail in their endeavour to talent-spot leaders in the making. Of this, the Nobel Laureate wrote that "it was the first cognitive illusion I discovered" and termed the phenomenon 'the illusion of validity'.

Such biases appear more frequently than we would like to admit. The following example, shared by Palmer, shows us that we can work very hard at finding the right answer to a wrong question, but once we see the blind spot, it is possible to use the fundamentals of behavioural economics to correct our course:

"I worked with a credit union on a new rewards checking account. Their billboard said, 'Earn up to 1.26% APY on up to $25,000 in balances'. That's math that makes people tune out. I got them to reframe it as: 'Did your checking account pay you $315 last year?' They have the same numbers but are completely different. It is easy to say no and creates curiosity to learn more. That simple tweak, even if you didn't set the rate, gives you a lot of control over what people choose."

The trick, according to Palmer, is to consciously pivot away from ingrained mental conditioning. "If you don't spend time really understanding the problem, you build products, add features, and set prices people don't want, which won't move the needle. Especially in banking, you are often not your best customer. The curse of knowledge clouds how you think about the outside user experience. Looking for ways to get out of your own way to find what people want is key."

DO WHAT WORKS

Success requires that banks harness interventions that will break down the behavioural barriers and/or biases of the target demographic without curtailing their freedom to choose. In a recent paper published in *The Behavioral Economics Guide 2024* titled *From Mindless Consumer to Mindful Citizen: A Behavioral Lens Approach,* using the objective of increasing savings (see **Figure 1**), the authors illustrate how this growing science can be applied to become a game changer for society and financial institutions.

The paper unpacks the mechanics of these 'nudges' and how banks can utilise the fundamentals of behavioural economics to influence people towards different (and often, better) life choices. A summary of these six interventions is as follows:

+ **The Power of Now.** These are interventions that take advantage of opportune times to maximise impact including, but not limited to, incentives and commitment schemes that will increase the propensity of savings plans. Moreover, actions could be based on identifying timely moments when consumers are most receptive to changing their habits and consumption patterns. For instance, banking mobile apps could prompt users with investment opportunities as soon as they receive their salary deposits. The Power of Now actions could seek to incentivise sustainable choices by front-loading benefits (e.g. tax credits that provide immediate savings).

For example, the Save More Tomorrow programme, developed by behavioural economists Richard Thaler and Shlomo Benartzi, uses the knowledge of hyperbolic discounting – a cognitive bias where people tend to gravitate towards immediate, smaller rewards instead of delayed, larger rewards – for greater economic good by getting citizens to commit to saving a portion of each future income increase without feeling the pain of saving immediately.

+ **The Power of Norms.** This makes use of people's desires or the Power of Norms to drive them towards options that can yield greater financial sustainability and social benefit. It plays on the instinct that most people want to fit in with the various conventions followed by their peers, generation, fellow citizens, or role models. Through awareness and open communication, it is possible to change the social narrative around expectations and nudge people away from a life of excess and high consumption and towards different values, including mindful consumption. Whether through

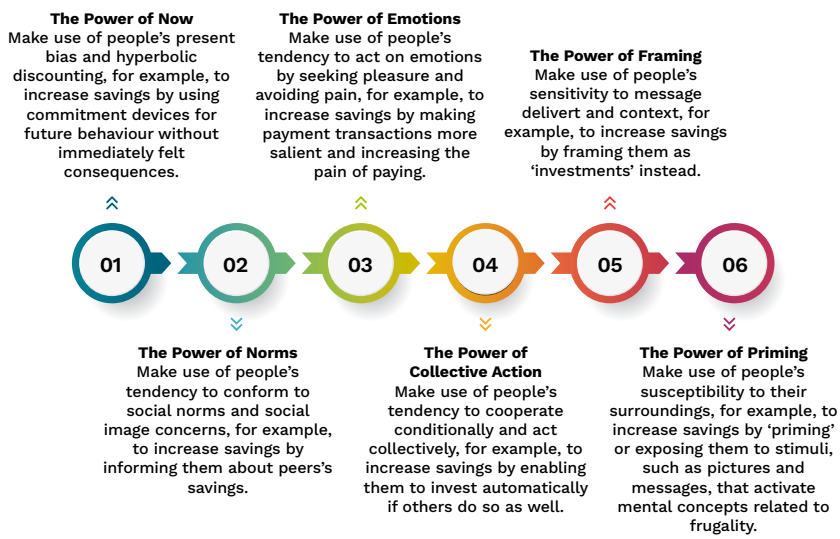


Figure 1 Potential behavioural interventions to increase savings.
Source: *The Behavioral Economics Guide 2024,* Behavioral Science Solutions Ltd, 2024.

the use of social influencers or harnessing media, this concerted effort to normalise savings and investment programmes can be embedded into popular culture and everyday conversation.

+ **The Power of Emotions.** Such interventions cultivate the desired behaviour by increasing positive feelings surrounding the end objective, such as increased savings and mindful consumption, whilst also making the negative emotions associated with the opposite objective more prominent. This can come in many forms and should be a two-pronged approach in order to obtain its maximum effectiveness. When people indulge in the desired target behaviour, there must be a systematic process which affirms the feel-good factor as well as a process to supplant any feelings of inadequacy in individuals who choose to go 'against the grain'. For instance, to strengthen negative emotions associated with mindless spending, the financial impact of spending in general can be made more salient. For example, a Swiss smartphone app used an emotion-based approach to highlight credit card transactions, making users more mindful of cashless spending.

Such interventions cultivate the desired behaviour by **INCREASING POSITIVE FEELINGS SURROUNDING THE END OBJECTIVE,** such as increased savings and mindful consumption, whilst also making the negative emotions associated with the opposite objective more prominent.

+ **The Power of Collective Action.** People's actions as consumers often lean toward selfishness. To counter this, mechanisms for conditional cooperation and collective action can help. For example, in the context of offsetting CO_2 emissions, instead of offering people the opportunity to pay to offset their individual emissions, the offer could instead be a call to action – the chance to offset carbon emissions can happen only if enough people collectively do so.
+ **The Power of Framing.** Framing, or how a message is presented, is known to cause large differences in people's reactions to a message. Leading research from the Behavioural Insights Team has shown how reframing 'savings' as 'investments' was found to increase suggested pension savings by 33% among young people. Using this knowledge to reframe certain messages or change how people think about specific choices can lead to vastly different outcomes. Thus, reframing can be used to change people's perspectives and affect their choices as a result.
+ **The Power of Priming.** Priming, or exposing people to a stimulus to temporarily activate specific mental concepts, can be an effective way to influence people's behaviour in a passive or even hidden manner. For example, research has found that exposure to art leads to less interest in status-oriented consumption by inducing a more meaningful, deeper state of transcendence.

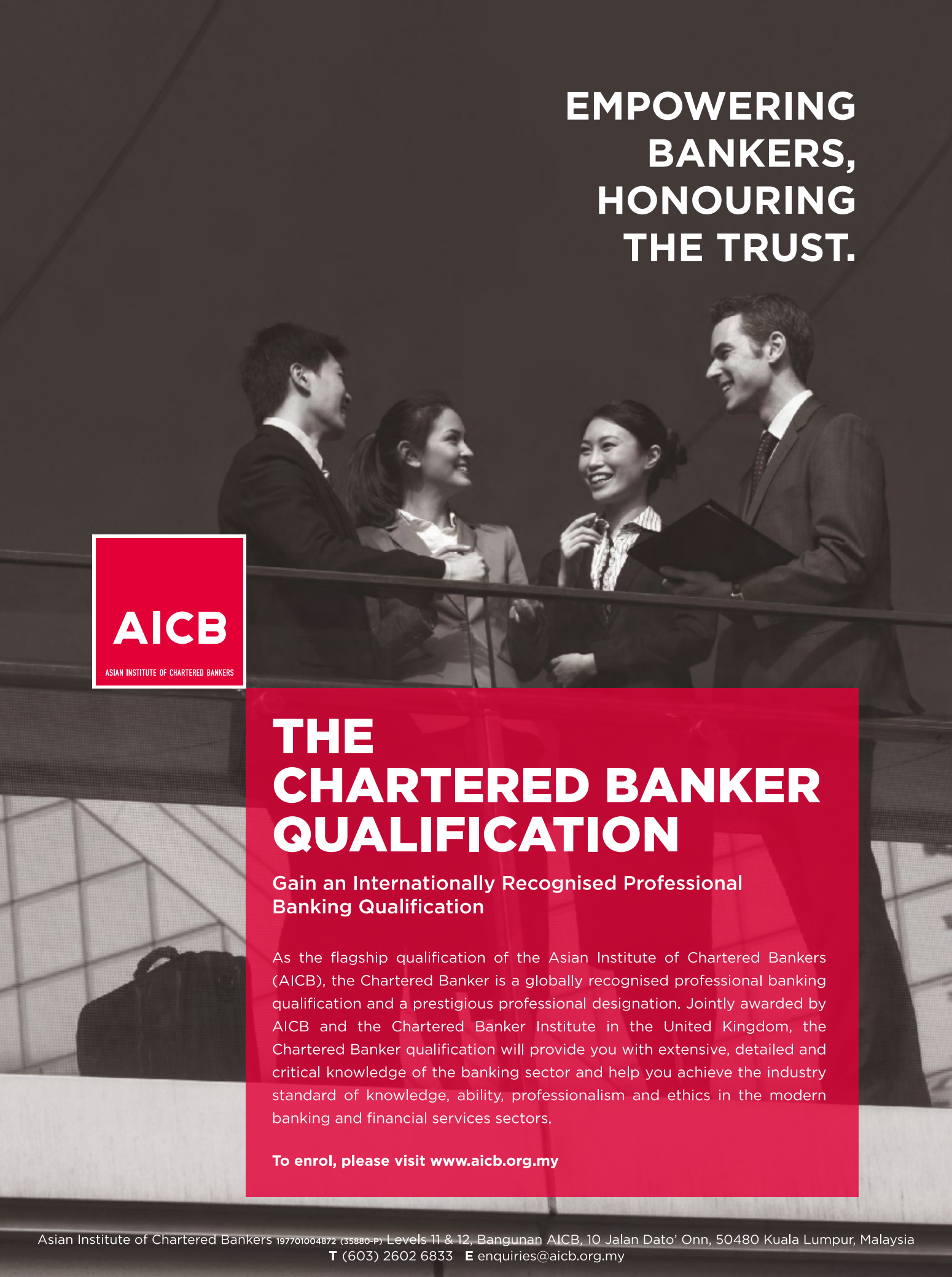
PROMPT DECISION-MAKING

Coming back to her point, Palmer concludes that there are "many paths with those 35,000 decisions going different ways…understanding how time matters to people is one."

"We're all victims to time discounting," she says, "what I call the 'I'll Start Monday' effect. Setting the alarm to run and then hitting snooze. We think of our future selves like a different person… bringing it to the now can be impactful."

Whatever their tools of choice, the end goal is for financial institutions to use the power of behavioural economics to drive future behaviour. Whether it is through more responsive ways of rate-setting or manipulating subconscious behaviours towards more sustainable choices, bankers must feel that they are psychologically empowered to approach these time-old problems in new and innovative ways. ✱

■ *Kannan Agarwal is a content analyst and writer at Akasaa, a boutique content development and consulting firm.*



EMPOWERING BANKERS, HONOURING THE TRUST.

AICB

ASIAN INSTITUTE OF CHARTERED BANKERS

THE CHARTERED BANKER QUALIFICATION

Gain an Internationally Recognised Professional Banking Qualification

As the flagship qualification of the Asian Institute of Chartered Bankers (AICB), the Chartered Banker is a globally recognised professional banking qualification and a prestigious professional designation. Jointly awarded by AICB and the Chartered Banker Institute in the United Kingdom, the Chartered Banker qualification will provide you with extensive, detailed and critical knowledge of the banking sector and help you achieve the industry standard of knowledge, ability, professionalism and ethics in the modern banking and financial services sectors.

To enrol, please visit www.aicb.org.my

Asian Institute of Chartered Bankers 197701004872 (35880-P) Levels 11 & 12, Bangunan AICB, 10 Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
T (603) 2602 6833 **E** enquiries@aicb.org.my