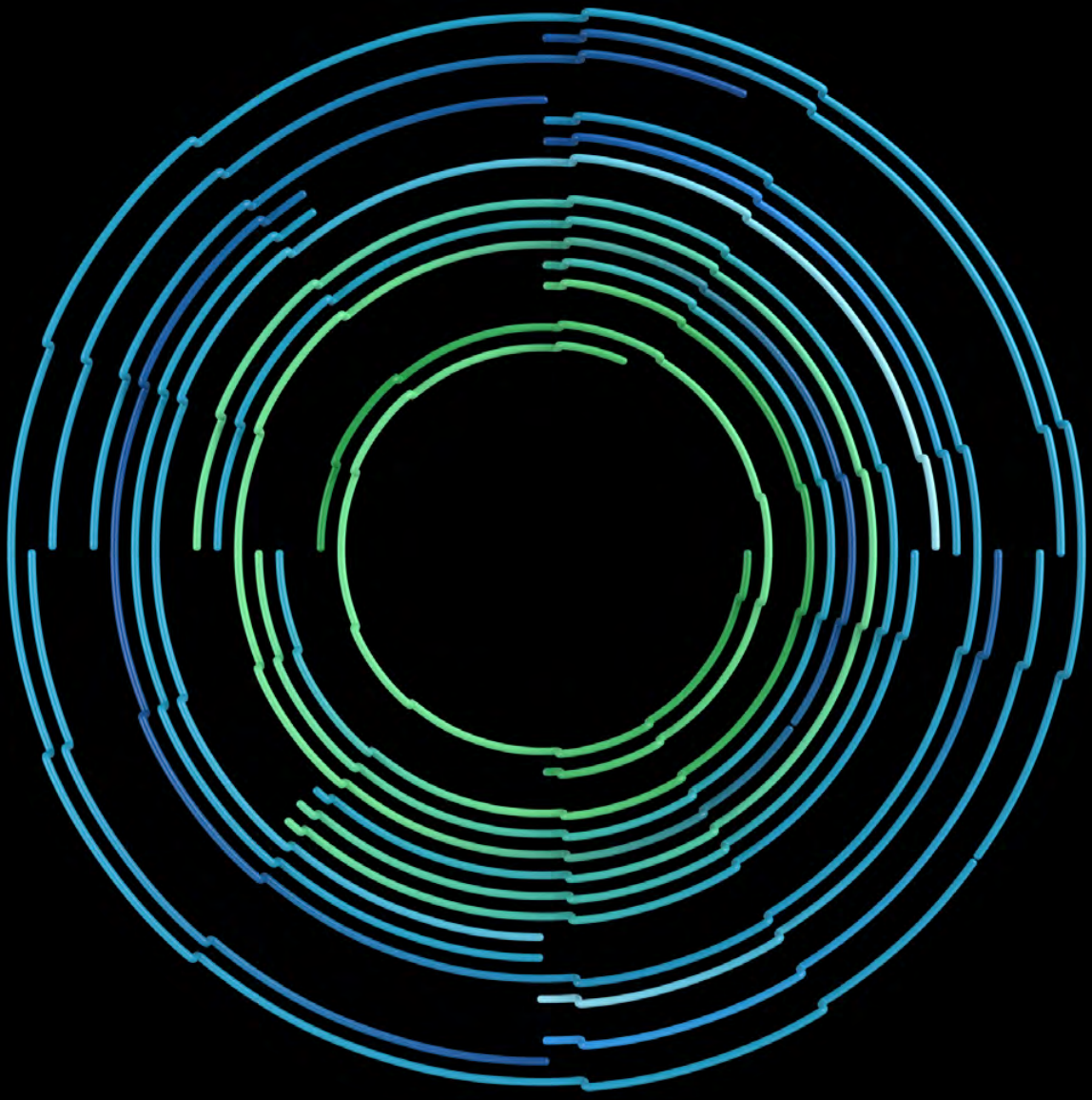
Deloitte.

UOB



The Future of Financial Crime Compliance

A Compelling Use of Innovation in a Converging Digital and Physical World

Volume 2

Forensic

Contents

Glossary of Terms

AI	–	Artificial Intelligence
AML	–	Anti-Money Laundering
AMLS	–	Anti-Money Laundering Suite
CFT	–	Counter Terrorist Financing
FCC	–	Financial Crime Compliance
FEAT	–	Promote Fairness, Ethics, Accountability and Transparency
FINTECH	–	Financial Technology
GDPR	–	General Data Protection Regulation
GFIN	–	Global Financial Innovation Network
KYC	–	Know Your Customer
MAS	–	Monetary Authority of Singapore
ML	–	Machine Learning
NLP	–	Natural Language Processing
PSD2	–	Payment Services Directive
POC	–	Proof of Concept
PPP	–	Public-private Partnerships
REGTECH	–	Regulatory Technology
RPA	–	Robotics Processing Automation
SAR	–	Suspicious Activity Report
STR	–	Suspicious Transaction Report
UOB	–	United Overseas Bank

Foreword

This whitepaper co-developed by Deloitte and United Overseas Bank ("UOB") examines how technological disruptions have transformed financial crime compliance.

It sets out the paramount need for the banking industry to enhance their compliance capabilities against the changing landscape of delivery of services and consumer behavior. The financial services sector has to tackle the compliance conundrum - manage profitability while keeping compliance top of mind. Increased competition from new entrants has also dialed up the need for financial institutions to accelerate innovation with new products and services.

Capturing and retaining customers remains a constant. Yet the evolving nature of banking competition and the onslaught of the fourth industry revolution that demands more innovative business models, together continue to push the boundaries of the future of financial crime compliance.

Much thought is warranted on whether compliance capabilities need to be reshaped since financial crime is a major risk for financial institutions. To continue to defend against financial crime, innovation by financial institutions to sharpen their capabilities remains key.

This whitepaper will first describe the criticality of the financial services sector's role in fighting financial crime. It would then list the manifold opportunities and considerations of using technology within financial crime compliance.

In the previous whitepaper[1] (Volume 1) entitled "The case for artificial intelligence in combating money laundering and terrorist financing", Deloitte and UOB started a journey to examine and share collective perspectives on the use of innovation to make financial crime compliance more effective. The use of Artificial Intelligence ("AI"), Machine Learning ("ML") and Robotics Process Automation ("RPA") was analysed, taking reference from UOB's collaboration with a Regulatory Technology (RegTech) solutions provider to develop a proof-of-concept (POC) for its Anti-Money Laundering systems and test it in a sandbox environment within the Bank. The pilot was a success. It resulted in greater accuracy in identifying suspicious accounts and transactions. The solution's ability to reduce false positive alerts enabled UOB compliance officers to streamline their investigations of suspicious cases and use the time saved on higher-value work.

One year on, this second volume examines the continued journey of UOB to shift the dial in financial crime compliance.

UOB is using next-generation technologies in the area of financial crime compliance to develop innovative solutions that meet business and regulatory needs. We will delve into the Bank's strategy in ensuring financial crime compliance in this paper.

The Future of Financial Crime Compliance | Foreword

Cheng Pui Yuen
CEO, Deloitte Singapore

"Technology is changing the way companies operate. With convergence and the blurring of lines between physical and digital products and services in the financial services sector, interesting questions are being raised about the future of compliance. What kind of operational framework and culture needs to be set, and what investments need to be made? How can the industry leverage innovative technologies to address the issue of financial crime better? All of this presents an opportunity to explore new dimensions and ways of doing things. This whitepaper paints a picture of what is to come, and Singapore, on its Smart Nation journey, will benefit from industry collaboration and co-creation that can bring broader confidence when navigating the future."

Victor Ngo
Head of Group Compliance, UOB

"In an increasingly complex regulatory landscape, banks must continue to ensure a strong compliance culture to safeguard customers' interest and to maintain the trust that stakeholders place in us. It is important to remain constantly vigilant to ensure that we stay ahead of new risks that are emerging every day, especially in an increasingly digital world. The digital age also offers opportunities for technological innovation that enables financial institutions to enhance our preventive, detective and enforcement measures and to sharpen our risk management model. This whitepaper reflects our learnings and experiences as we developed a compliance strategy that taps new technologies to enhance our risk management practices and to defend against financial crimes today and in the future."

Introduction

A disrupted new world in financial services

While the financial services sector faces an array of risks today, there is perhaps none as disconcerting as the impact of financial crime risk.

The trillion-dollar threat has far-reaching consequences and combating it is an unenviable task for every participant in the global financial economy. Notably, the issue of financial crime is a common challenge faced by both large and small financial institutions. Substantial regulatory fines, ballooning compliance costs, and reputational impact are high-stakes across all financial institutions.

While the existing financial crime compliance model driven by rules-based algorithms is still relevant today, there is an urgent call to respond to the shifting expectations that regulators place on financial institutions to prevent, detect, and predict illicit money flows. The issue is exacerbated when legacy methods, disjointed operational frameworks and financial crime controls remain unchanged despite criminal sophistication. Traditional monitoring technology, even when optimised, falls short – it cannot always focus on what matters most, and still continues to generate too many false positives.

New risk complexities contributed to by shifts in the business landscape and regulatory expectations require a refreshed approach of uplifting standards, surveillance capabilities, controls, internal policies and procedures. In essence, the changing landscape not just necessitates business transformation but also compliance transformation.

Success will be driven by the seamless integration of business strategy, regulatory compliance, risk management, technology, and operations.

Financial institutions should reexamine their risk management function, including the ownership roles and key responsibilities of the first two lines of defense.

While there is no silver bullet to fighting financial crime, new and better compliance frameworks and controls will enable financial institutions to stay ahead of criminals and money launderers.

The Future of Financial Crime Compliance | Introduction

"Innovation in financial crime compliance to deploy the use of AI, ML and RPA is, today, a basic need for financial institutions to monitor risks and threats in a sharp and judicious manner. As next steps, we believe that innovation has to move a few notches up to monitor and assess financial crime from a holistic perspective for an enhanced view of material risks – both internal and external. As the following imminent step, we call for a public private partnership to create industry level utilities to undertake surveillance on transactions, typologies and threats in a more seamless fashion powered by innovative technological capabilities. Silo view of risks through the infrastructure of a single financial institution may not provide the outcome required in this fast changing environment, be it the emerging business landscape or financial crime sophistication. The burden placed on financial institutions has to tip to a more rationalised balance with the sharing of responsibility by numerous stakeholders."

Radish Singh
Southeast Asia Financial Crime Compliance Leader and AML Partner,
Deloitte Financial Advisory, Forensic, Deloitte

Chapter 1:

A closer look at key trends in financial crime compliance

Perspectives on how the digital revolution is reshaping financial services

The Future of Financial Crime Compliance | Chapter 1: A closer look at key trends in financial crime compliance

In 2018, financial institutions globally planned to invest US$9.7 billion in enhancing their digital banking capabilities in the front office.[2] While financial institutions race to remain competitive by investing in digital technologies that enhance services and solutions for the customer, equal attention needs to be given to mitigate multi-faceted financial crime risks.

This chapter examines the latest trends in the digital revolution and their potential financial crime risks.

First, the arrival of digital and virtual banks and non-traditional platforms. In Europe, digital banking has become mainstream, propelled by customer demands, and subsequently governed by the revised Payment Services Directive (PSD2). This key regulatory initiative of the European Union aims to facilitate innovation and competition by creating a level playing field for financial institutions, emerging Financial Technologies ("FinTechs") and other third parties.[3] To date, European regulators continue to pioneer in this space via the Global Financial Innovation Network ("GFIN"). GFIN is a global innovation sandbox set up in early 2018 for FinTech firms seeking regulatory insight to test and scale products and services in a regulated environment and is supported by 35 financial services regulators.[4]

In Asia, digital banking is not new either. The arrival of such virtual licenses in Asia to disrupt brick-and-mortar banking started in the early 2000s with Japan, China, and South Korea. In 2019, Hong Kong has also granted virtual banking licenses to eight companies.

More recently, Singapore has joined the foray, offering five new digital bank licenses that will drive intensified competition between banks and non-bank companies Marking this move as the "next chapter in Singapore's banking liberalisation journey", the Monetary Authority of Singapore ("MAS") has enlarged the banking and finance sector to "ensure a competitive and growing centre for finance in Asia and globally".[5]

Digital banks have brought about new customer experiences. The shift from brick-and-mortar bank branches to online and omni-channel banking services has also brought about faster go-to-market and delivery of financial services.

With the rapid change pressing in on them, brick-and-mortar banks are now also making swift changes toward digitising their delivery platforms and channels. While improving customer experience, digital banks have also introduced additional financial crime dimensions. Digital banks are typically branch-less, with easier handling and anonymous cross-border transfers that causes more complex transaction monitoring for financial institutions and authorities.

Also, technological innovations by traditional banks will require appropriate regulations to supervise and monitor the new business models that bring opportunities but also new risks when there are regulatory gaps and loopholes.

Given the shift towards digital transformation, the vulnerabilities for financial crime continue to manifest in cross-border transactions and the interconnectivity between multiple economies that are governed by a varied spectrum of lax to stringent regulatory requirements.

Whatever the case, the baseline expectations of the regulators is that financial institutions must ensure that there is market integrity, effective customer due diligence processes and on-going monitoring, specifically with regard to AML and CFT risks.

As a consequence, in a digital or virtual banking model, the financial crime compliance dimension is on the cusp of transformation.

Regardless of the delivery channel, financial crime risk has to be managed and must be done in a manner commensurate with the business model, product vulnerabilities and services to risks.

Traditional Know-Your- Customer ("KYC") processes will have to be reimagined and accelerated. This is because customers are receiving round-the-clock digital services bypassing human interaction to the extent possible. These advances bring benefits but also next complexity. While faster onboarding is to be expected from branchless banking, AML/CFT background checks and underlying customer due diligence still require particular attention in assessing potential risks.

Financial crime compliance must continue to be placed at the fore. For example, UOB's first mobile-only bank - TMRW - is seeking not merely to offer a differentiated customer experience to millennials, but to protect the customer's interest and mitigate risks to the banking system.

TMRW was launched in its first ASEAN market - Thailand - in March 2019.[6]

To support the business model for its digital bank without compromising its robust compliance controls, UOB first identified the portfolio of risks for TMRW. The Bank then determined how to ensure financial crime compliance for the digital bank.

Second, the arrival of non-banks and payment providers (FinTechs) that offer more accessible and convenient payment alternatives. Growth in the payments space are driven largely by a renewed focus on customer centricity, offering a plethora of payment options including digital wallets, mobile wallets, crossborder payments, cryptocurrencies (token and exchanges) that reduce payment friction and support transactions. These payment methods bring forth new financial crime risks that could mean new regulations may be required to address them.

For example, cryptocurrencies and their potential abuse as a means to finance terrorism is a significant threat, especially when its anonymous nature and lack of regulatory supervision could be exploited.

The point is clear: As much as financial institutions and financial technologies ("FinTechs") are experimenting with new models to offer faster "time to market", and cost efficient products and services, bad actors are finding smarter ways to launder ill-gotten gains. At the same time, boundaries will be pushed to ensure that more effective systems emerge constantly to combat financial crime.

In Singapore, the Payment Services Bill that was recently passed brings all payments services under a single legislation to take into account new developments and the various risks they pose to AML and Counter Terrorism Financing ("CFT").[7]

Singapore is one of the first countries in the world to introduce a new licensing regime that finely balances the promotion of digital payment innovations with the mitigation of risks. With the Bill, payment providers and exchanges will have to consider AML and CFT risk, though this will be imposed within appropriate levels, to avoid onerous or stifling regulatory burden.

In any case, the introduction of a new regulatory framework for digital payment services is a positive response to the latest innovation and business models in the industry.

Third, faster payments. As previously mentioned, the banking industry continues to be transformed by rising consumer expectations to manage and move money with greater flexibility and speed. Modernising payments yields growth benefits for businesses such as those in the areas of money remittance and e-commerce since it ultimately improves customer experience and helps accelerate business transactions.

Further, enabled by technology innovations, moving money at high speed and across borders has become much easier. This has also introduced new pressures and expectations on AML and CFT compliance.

With current models of AML compliance, delaying transactions to ensure proper review and KYC checks will directly affect these sought after efficiencies that are expected by customers. Faster payments gives little time for monitoring and could invoke considerable pain points within a financial institution's front and middle office operations and capabilities.

Financial institutions keen to be part of the digital arms race will find that the early establishment of best practices and compliance risk management is crucial.

The Future of Financial Crime Compliance | Chapter 1: A closer look at key trends in financial crime compliance

"Banking goes beyond technology; FinTech firms must ensure that they have all the elements and responsibilities of risk management and regulatory compliance in place to offer banking services."

Dennis Khoo
Regional Head of
TMRW Digital Group, UOB
The Business Times, 08 May 2019

Chapter 2:

Toward a new financial crime compliance paradigm

Perspectives on mixing smart technology in a converging digital and physical world

The Future of Financial Crime Compliance | Chapter 2: Toward a new financial crime compliance paradigm

Traditional Approach

The traditional framework (See Figure 1) for financial crime compliance is a labyrinth of policies, procedures and processes. This may have been of sound design and effectiveness prior to the change in landscape previously mentioned. However, to ensure that financial institutions remain effective against increasingly complex financial crime, there is a need to review legacy processes.

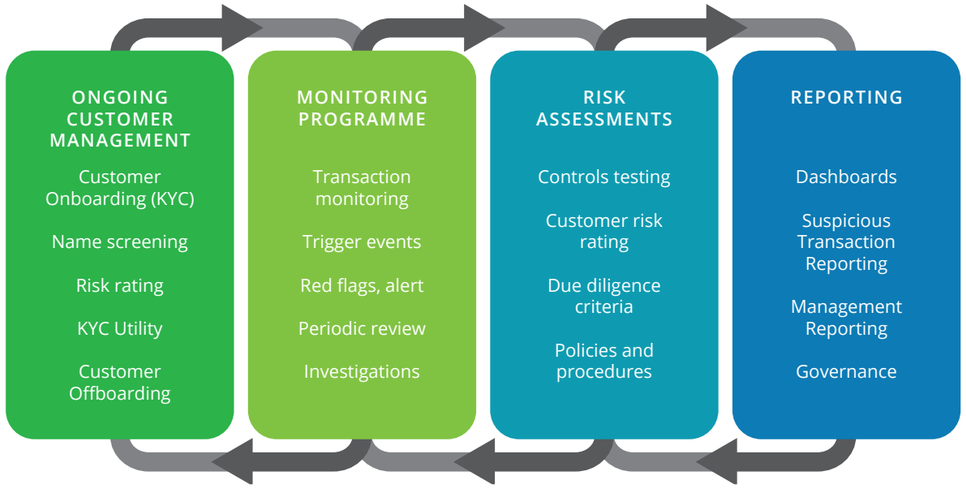
Such reviews could mean re-engineering legacy processes and design principles that typically operate in silo and contain cumbersome architecture. It could also mean revamping manual processes laden with associated challenges that include human error, lack of agility, and complex operating models.

Accordingly, a new approach that maps out the customer journey and the compliance processes is required to break siloes and to ensure that the necessary safeguards are in place across the business' portfolio of products and services. These compliance processes include KYC, Know Your Customer's Customer, enhanced due diligence, ongoing monitoring, name screening, transaction monitoring, assurance, risk assessments and reporting.

There are three phases of compliance programmes in our view:

- The first phase as explained is the traditional model;
- The second phase is the next-generation compliance framework where financial institutions innovate to connect AI/ML and RPA into key processes or technologies to become more effective in managing financial crime; and
- The third phase is moving a step further into a futuristic approach by undertaking holistic surveillance and analysing financial crime threats. This is yet to be tested.

Figure 1: Traditional Approach to Financial Crime Compliance



A New Approach

To execute this new approach, business units (first line of defence) and compliance functions (second line of defence) should agree upon the key threats that require monitoring, their representative controls, as well as risk owners. In the United States, the Federal Reserve Board's guidance sets the tone for business leads to be accountable to risk owners. Similarly in Singapore, MAS has provided guidance on the necessity of the Board and business leads to proactively manage money laundering and terrorist financing risk.[8] Consequently, implementation of controls has to be driven by the business with advice from compliance.

In line with this guidance, a robust and comprehensive roadmap to deploy the initiative must be formulated. This means the first line of defense will have to play a critical role in understanding regulatory obligations and work closely with compliance to ensure proper risk mitigating measures with the right controls are in place.

With financial crime compliance seen as a Board Agenda, collaboration between the two lines of defense should set a strong compliance culture and ensure that the interest of financial institutions and their customers is safeguarded and sustained over time.

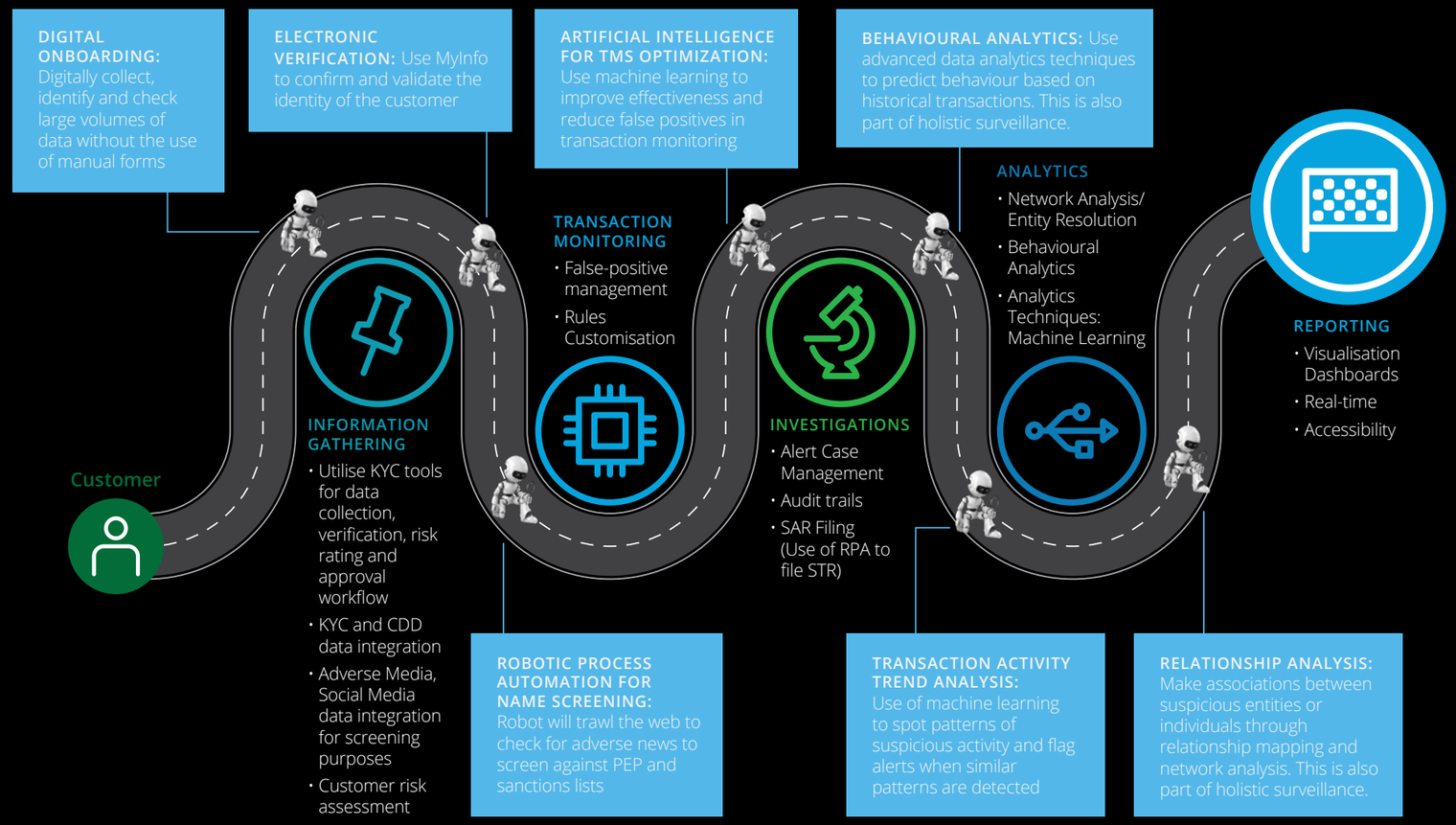
Across the financial crime risk management framework, there are many areas in the value-chain where technological innovations such as data analytics, AI, ML, RPA, Natural Language Processing ("Natural Language Processing") and cognitive intelligence can be applied.

No two financial institutions will adopt technologies in the same manner. Such endeavours are largely dependent on the firm's vision, short, medium and long-term goals, limitations, and risk appetite for digital transformation.

Using technologies across the customer lifecycle

Key opportunities for innovation and the use of technology and analytics to curb financial crime in every step

Figure 2: Deloitte view of new generation compliance framework where financial institutions innovate to interlace AI/ML and RPA into key processes



As with most transformation projects, the inner workings within operational frameworks anchor its outcomes and successes.

The journey requires a closer look into technological design and implementation. This includes addressing key aspects such as:

- Data quality and data mining in a new era of data privacy from the implemented EU General Data Protection Regulation ("GDPR") and Singapore's principles to Promote Fairness, Ethics, Accountability and Transparency ("FEAT")
- Integrating multi-source data and data security
- Governance of complex technologies such as AI and ML
- Hybrid workforce: Human talent, machines and skills of the future

Every aspect is required to manage and deploy technologies against compliance requirements and the desired business outcomes. Compliance, data scientists and IT teams play a critical role in assessing and organising the approach to attain the required objectives.

Singapore's Push to be a Smart Financial Centre

In January 2019, the Singapore Government released a guide entitled "The Model AI Governance Framework", for organisations to practically address key ethical and governance issues when deploying AI technologies.[9]

Specifically, it looks at four key priority areas:

I. Internal AI governance structures and measures;

II. Risk management in autonomous decision-making;

III. Operations management; and

IV. Customer Relationship Management

Singapore's laser focus on AI governance has provided much needed guidance that has provided clarification to financial institutions and compliance practitioners to consider the governing principles when it comes to the promises of using AI.

As with all broad adoption exercises, concerns around governance, documentation, relevant talents and resources to handle complex enterprise technologies emerge.

Furthermore, regulators may also have a greater level of expectation in the production and adoption of AI models. Greater focus is required to first develop a sound and structured approach before the testing of these models. Existing risks reside in:

- data privacy and protection regulations breaches (e.g. GDPR, PDPA, FEAT),
- defensibility of outcomes,
- unclear or conflicting regulations,
- lack of standards and regulations,
- lack of audit trail and traceability.

In line with the authorities' views, the transition to a comprehensive future financial crime compliance model in the mid to long term should aim to feature a holistic, continuous and intelligent view of a financial institution's entire financial crime risk landscape. To do so, there must be the proficient use and analysis of data sources from multiple channels and the pinpointing of financial crime risks with greater confidence through the combined expertise of financial crime compliance experts and next generation technologies. This will include analysing both internal and external threats that can pose a risk to the financial institution.

By doing so, we aspire for this to also provide financial institutions with enhanced capabilities for early detection, taking preventative measures and reporting anomalies and suspicious activities in a timely and swift manner.

The Future of Financial Crime Compliance | Chapter 2: Toward a new financial crime compliance paradigm

Transitioning to a foreseeable Future State of Financial Crime Compliance

The design of the future state, we believe, must include the following considerations:

1. **Public-private partnership and sharing information.** For example, KYC utilities at the national level could evaluate data and intel from various sources to profile a customer including using entity resolution to understand any linkages to risk rate customers. The manner in which periodic review is undertaken must be innovated with cutting-edge technology capabilities. This would be more meaningful than the collection of a myriad of documents that damages the experience of the genuine customer.

2. **Onboarding customers based on their profile and susceptibility to financial crime threat rather than making broad-stroke guesses at customer risk based on straightjacketed indicia.** The latter is losing its charm in the world of increased complexity that demands cogent evidence based information.

3. **Screening and monitoring transactions with the use of AI and ML models to assess real threats rather than using rigid rules that result a large volume of false positives.** This process should be embedded with an automated assurance functionality built into the framework through the use of technology. We anticipate that such an endeavour will result in providing a view around the defensiveness of the models being used and an overall effectiveness and efficiency. The ultimate goal should be for industry level untilities to undertake transaction surveillance;

4. **Use of digital platform to conduct first, second and third line assurance,** risk assessments and threat based analysis of risks from the data made available from all sources. The calculation of inherent risk should take into account data relating to the real financial crime threats posed to the financial institution. This should inform the focus of first and second line assurance programme. Risk and controls effectiveness should be viewed from a single assurance platform by understanding the weaknesses found across the organisation via various assurance programmes and analysis undertaken for products and services, risk assessments, KYC, screening and monitoring with AI / ML, etc.

5. **Use of RPA and digitisation across all reporting demands** that includes both internal and external reports, thereby minimising manual work involved in producing myriad of reports. The use of RPA should also bring ease in drawing out potential linkages and themes which could be easily missed in manual reporting.

6. **Undertaking holistic surveillance to close the loop in ensuring that no material risks go unnoticed.**

Figure 3 is a simplified illustration of a Deloitte holistic surveillance model and blueprint.

In our view, holistic surveillance mechanism should use data from all relevant sources within the financial institution to transform the visualisation of financial crime risks. It is our expectation that holistic surveillance will allow financial institutions to monitor and focus on key risks. It will provide early warning signs for taking preventative measures, a picture of where risks are concentrated within the organisation and sharpen focus on material threats posed to the organisation based on all data sources.

In designing this, we are looking into the use of AI and ML models to learn and assess threats, data analytics to visualise risks and contextualise data for relevance to financial crime risks.

We intend to report on the outcome of this approach in the near future.

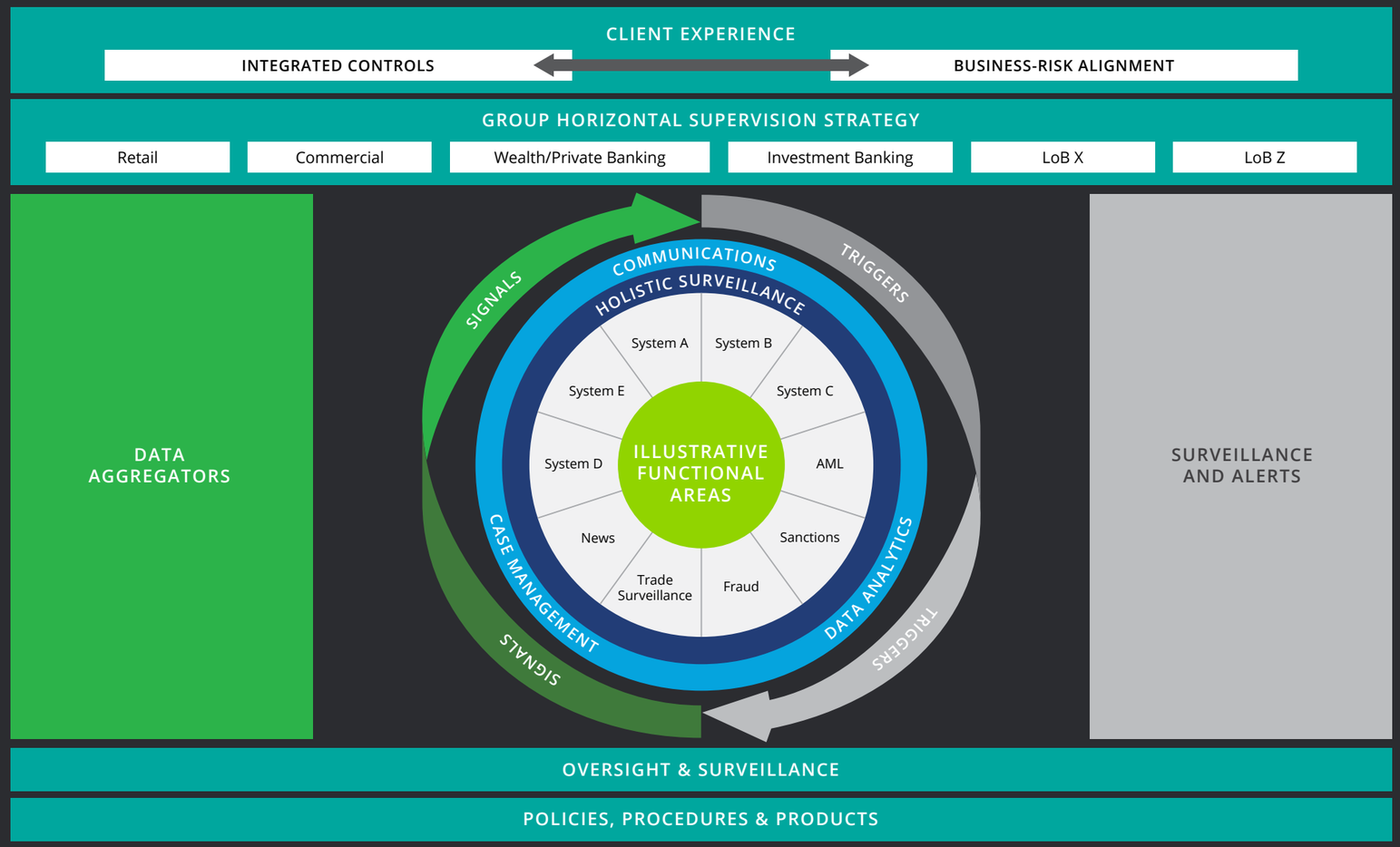


Figure 3: Deloitte's blueprint for a holistic surveillance model. Note that this is the intellectual property of Deloitte Touche Tohmatsu Services, Inc. and should not be copied or reproduced without prior written consent or permission from Deloitte.

Challenges of the Holistic Surveillance Approach

The use of cutting-edge innovation and treading into unchartered territory requires management commitment.

Accordingly, key challenges are:

- Seeking internal "buy-in". This is not easy when dealing with what seems like a blue-sky concept with no tangible credentials and data points;
- Sandboxing and incubating new ideas to create the test environment. Working towards the target state requires sponsorship, time and resources;
- Ensuring that the incubation results in a metamorphosis of deployable results. The pressure to succeed has to be balanced with good governance, planning, reasonable timelines, troubleshooting issues due to data and legacy systems. Testing and assurance will also require a defensible approach that can be operationalised, explained and able to withstand challenges;
- Selecting the right partners through a robust selection process; and
- The lack of an eco-system makes the journey even more precarious and vulnerable from a sustainability perspective.

Chapter 3:

UOB's Journey: Today's Edge, Tomorrow's Advantage

United Overseas Bank Limited (UOB or the Bank) is upholding its commitment to be a Bank with a strong risk-focused culture using next-generation technologies to stay vigilant in an ever-changing financial crime landscape.

The Future of Financial Crime Compliance | Chapter 3: UOB's Journey: Today's Edge, Tomorrow's Advantage

UOB's Financial Crime Compliance Approach

As part of its strong focus on maintaining a risk-focused organisational culture, UOB is partnering with technology innovators and industry leaders to enhance its compliance capabilities to stay ahead of emerging risks. In the area of financial crime compliance, UOB has created an 'AML/CFT Technology Roadmap' to harness next-generation AI and ML driven technologies to combat money laundering and terrorist financing.

Several factors were considered in the implementation of this roadmap. The Bank reviewed the plethora of RegTech solutions which could be suitable for the Bank's needs based on their agility and scalability, their interoperability with existing IT infrastructure to implement AML, CFT and Sanctions controls. In addition, the selection of best-fit technologies had to meet investment returns objectives, tangible benefits and outcomes, and most importantly, drive business performance and enable the Bank's business units to enhance the way in which they serve customers. The Bank is also building ML models in parallel to its existing rules-based AML systems. The aspiration is to shift beyond rules-based systems to achieve higher performance with ML models and other disciplines of AI.

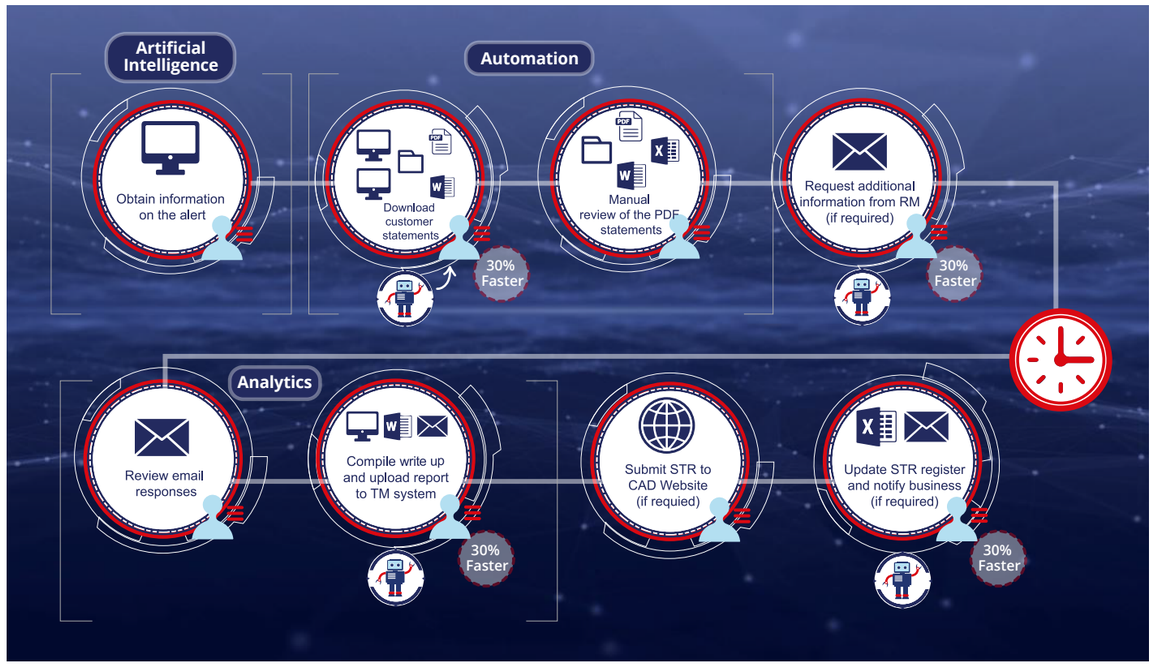
The ways in which financial crimes are being committed continue to change and a holistic view of risks and the threat-scape is important. UOB's 'Triple-A approach' (see Figure 4) taps AI, Automation and Analytics to enable the Bank to stay ahead of financial crime and to make sharper, smarter and swifter detection of high-risk activities. The Bank also expanded its team of experts with skills and experience in data and AI. Deloitte worked alongside the Bank as a knowledge partner across their AI and Automation processes.

To evaluate suitable RegTech that could drive the Bank's compliance objectives, UOB identified two areas in financial crime compliance - transaction monitoring and name screening - to test new innovations. UOB will then implement successful innovations that align with its compliance strategy across the Bank. The adoption of the 'Triple-A approach' and the promising results in triaging, classifying and ultimately focusing on what is material will be discussed in the rest of this chapter.

In particular:

1. **Inside UOB's AI Journey: Realising the vision to implement AI**
2. **A winning mix of Automation and human resources**
3. **Pushing the boundaries of insight with Analytics**

Figure 4: UOB's 'Triple-A approach' for transaction monitoring



1

Inside UOB's AI Journey: Realising the vision to implement AI

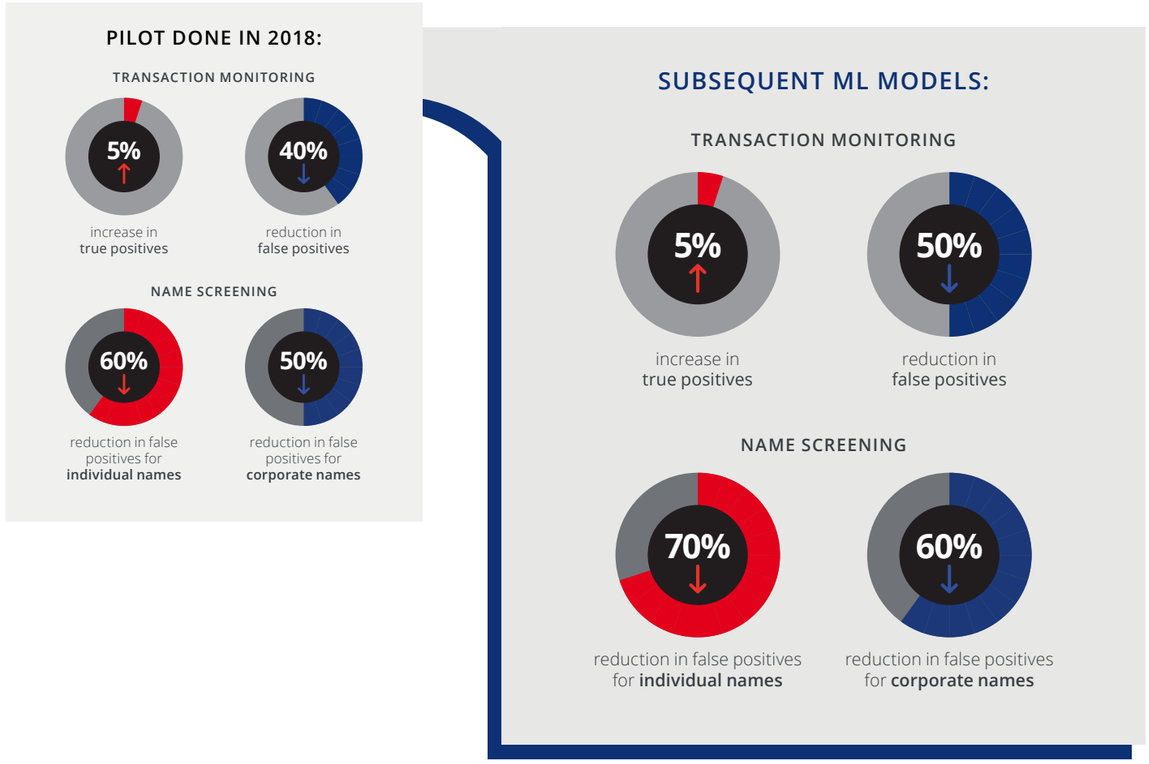
The pilot of ML models to combat against money launderers and terrorist financing is in full swing with the Bank moving towards production.

In 2018, UOB teamed up with Tookitaki, a Singapore-based RegTech startup to use ML as part of its anti-money laundering programme. Tookitaki's Anti-Money Laundering Suite ("AMLS") is an end-to-end transaction monitoring and name screening system. It combines supervised and unsupervised ML techniques that seeks to detect suspicious activities and identify high-risk clients quicker and more accurately. In the 2018 pilot, Deloitte performed an independent model validation, conducting reviews and validation techniques to assess the conceptual soundness of the Bank's ML models. The results are detailed in a case study entitled 'UOB, Tookitaki and Deloitte readies machine learning pilot to accelerate the fight against money laundering' found in Volume 1 of a joint whitepaper between UOB and Deloitte.

The results of the 2018 pilot and the subsequent ML models are illustrated in the diagrams below:

The subsequent ML models were tested with a unique data set, yet they achieved a 50 percent drop in false positives for **transaction monitoring** processes compared to the 2018 pilot that was 40 percent. Similarly, for **name screening** processes, the subsequent ML models fared positively with a 70 percent reduction in false positives for individual names and 60 percent reduction in false positives for corporate names.

The successful results gave UOB the confidence to begin its next phase - moving the ML models to production. However, prior to this, the Bank will go through another round of model validation to ascertain the robustness of the models.



"We are excited to be one of the very few RegTech companies globally to operationalise a machine learning-powered anti-money laundering (AML) solution within a bank's existing infrastructure. Tookitaki's Anti-Money Laundering Suite (AMLS) uses a combination of distributed data-parallel architecture and machine learning to ensure scalability across a bank's multiple business lines and complex layers of existing technologies and systems.

High model accuracy, continuous learning, detailed explanation of outputs and easy integration with a bank's upstream and downstream systems make AMLS an optimal choice for any sustainable AML compliance programme designed to scale.

Nevertheless, the successful deployment in production environment lies in a coordinated effort between the software vendor and the bank's technology, AML compliance, internal audit and model validation teams."

Mr Abhishek Chatterjee
Founder & CEO, Tookitaki

Today, the Bank is actively working with Deloitte and Tookitaki to prepare for its pre-production and production environment to launch the ML models.

Tangible benefits observed using ML models for AML compliance:

- Increased effectiveness in identifying suspicious activities
- Sharper focus on data anomalies rather than depending on threshold triggering
- Easier customisation of data features to target specific risks accurately
- Enable longer look-back periods to detect complex scenarios

Tookitaki

- AMLS solution received the 'AI in Banking' Excellence Award from the Singapore Business Review[10]
- AMLS solution selected as one of the World Economic Forum's 'Technoloy Pioneer Cohort 2019'[11]
- AMLS solution wins the 2019 SG:D Techblazer Award (silver) in the most promising innovation category

Pre-production Preparations

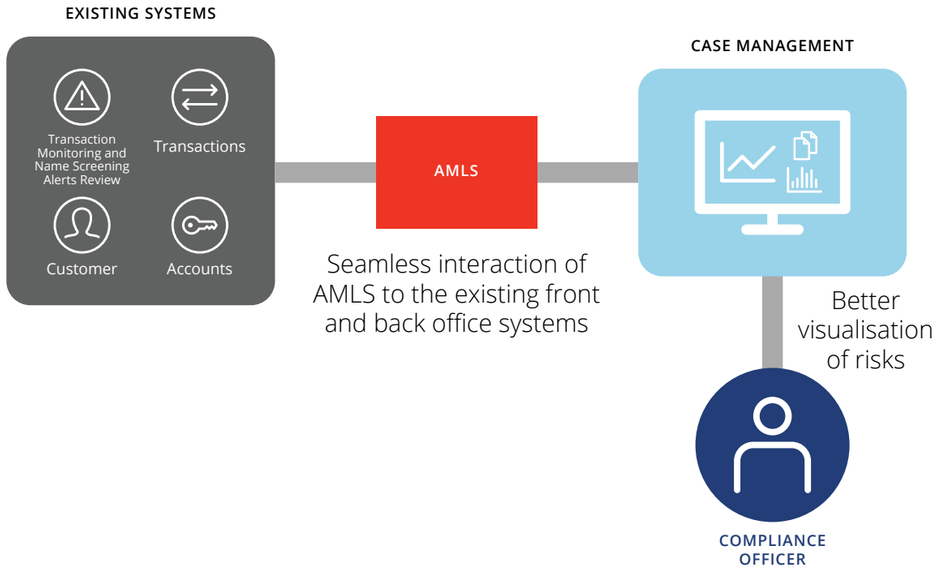
In this step, the considerations amplify as new risk factors arise. These issues have to be resolved before the models can be scaled across the Bank's multiple business lines and complex layers of infrastructure and systems.

Operationalise

To operationalise the AMLS, additional assurance and testing for model confidence on real-data sets are being done to ensure it can integrate with the Bank's current infrastructure well. Considerations such as data management, privacy and data issues, and the need for the right sets of skillsets and capabilities to supervise models are also part and parcel of what it means to put the ML models into production.

The Bank is working with Tookitaki to address these outlined considerations pursuant to the validation exercise undertaken by Deloitte. In terms of the integration of AMLS with existing technologies and systems in the Bank, key steps were planned to ensure that the additional layer of the AMLS has no disruptions to normal business processes and activities. With the introduction of AMLS, the output files from alerts are built to be compatible with existing case management systems, so that compliance officers can easily access alerts and prioritise investigations. (See Figure 5). The advantage of having this approach meant that compliance teams were already familiar with the workflow for alerts management and minimal retraining is needed. The Bank is working toward a governance review and assurance process to ensure that low value alerts receive adequate attention. This is also in line with UOB's robust risk management approach.

Figure 5:



Governance

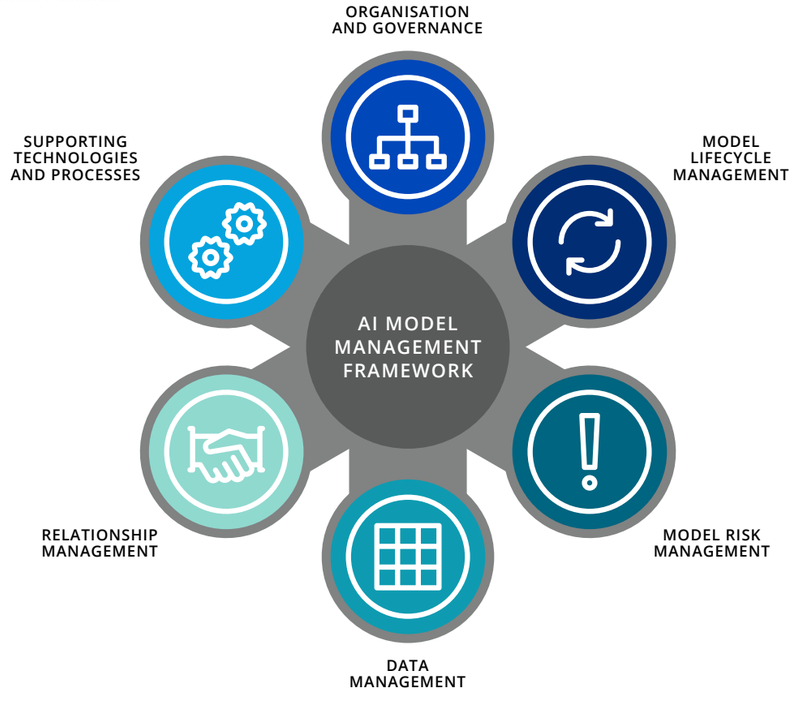
In the area of supervision and governance, the Bank has also adopted principles from Singapore's AI Model Framework when charting out practical steps to deploy AI at scale in financial crime compliance. UOB and Deloitte collaborated to develop a resilient governance 'AI Model Management Framework' (see Figure 6) in financial crime compliance. This formed the initial guiding approach for implementation of ML models that include model risk management, managing biases, explainability of the models, application of data privacy and FEAT principles, data management, assurance and testing of the models and incident resolution.

Continuous review of the receptiveness of these ML models through a well-structured feedback loop is an imperative. Ultimately, determination of threats and risks to the Bank depend on sound judgement of the human analyst. The latter is the collective aspiration of UOB and Deloitte and the aim is to involve a wider eco-system of participants that include regulators, RegTechs and the financial services sector.

Presently, the Bank is in the preparatory stages for production, reviewing operationalisation and governance design in order to fine-tune and scale the models with a structured approach. The launch of the first productionised ML models is currently slated for the first half of 2020.

These ML models will be layered onto UOB's existing AML systems to monitor transactions and conduct name screening. This means that even as the Bank deploy its AI and ML platform, it will also continue to optimise the existing rules-based systems.

Figure 6: AI Model Management Framework



Associated governance challenges when using ML models:

- **Human biases** that will affect ML models and algorithms. To the extent possible, human biases must be excluded for models. A delicate balance and due care is required to ensure that the removal of biases does not eliminate the typologies and red flag based monitoring that is an imperative in financial crime compliance.

- **Transparency concerns** and "black box" design. Regulators will not accept black boxes. All necessary effort must be dedicated to ensure explainability of models.

- **Misunderstood uses and technology** with the needs to demonstrate clearly the benefits of innovation in creating greater effectiveness in managing financial crime risks.

- **Misunderstood governance**, ethical challenges and applications. Regulators expect that the Board and Senior management remain on top of the innovation deployed in a financial institution. In addition, model risk management that challenges processes in order to provide assurance is necessary.

- **Controls** over supervised and unsupervised learning.

The Future of Financial Crime Compliance | Chapter 3: UOB's Journey: Today's Edge, Tomorrow's Advantage

"As a values-based bank, ensuring that we stand by our customers and do right by them is at the core of all that we do. UOB's compliance function work closely with the Bank's technology and operations teams and business segments to maintain our robust compliance controls and to keep pace with the changing industry landscape. Together we ensure a strong risk culture within the Bank that complements our innovation drive to design solutions and services that matter to our customers."

Victor Ngo
Head of Group Compliance, UOB
IBF Distinguished Fellow (2019)

2

A winning mix of Automation and human resources

Maintaining regulatory compliance can be an uphill task; and is exacerbated where organisations continue to deploy fragmented and manual processes when conducting financial crime compliance activities. Given the numerous data points, extraction and synchronisation of files, reports and workflows, using RPA serves as an effective and useful tool to improve regulatory compliance. Specifically, automation opportunities abound such as name screening, transaction monitoring alert clearance, and SAR/STR reporting. These processes are repeatable and/or routine, rules-based, and can be performed with minimal human interference and best suited for RPA.

For example, the traditional approach for name screening in KYC remediation is highly manual, repetitive and resource heavy. With RPA, scale and value is achievable with greater assurance, lower cost and higher speed of execution. The use of such robots are growing with considerable interests as tangible benefits are observed, particularly in terms of:

- Productivity: Robots can operate 24/7/365
- Efficiency, Quality and Accuracy: Humans are prone to manual errors especially with voluminous alerts that are routine and onerous.
- Time and Cost Saving: Robots can be scaled to meet peak demands and takeover rules-based administrative tasks

"It is a continualjourney for us. Our priority is to ensure that all investments have a tangible outcome and can be scaled across the Bank after the proof of concept. As a result, we would rather spend a longer time thinking through the business case and working with the right partners to help us focus on what's possible within the context of UOB rather than open experimentation. At the end of day, we want something that is best suited to the needs of our bank and sustainable for the long term."

Victor Ngo
Head of Group Compliance, UOB
IBF Distinguished Fellow (2019)

As part of UOB's automation efforts, Deloitte assisted with the implementation of RPA to help improve a number of selected processes within the Bank's transaction-monitoring framework. These include alert review tracking, alerts review, alerts allocation, and STR upload and listing.

These select processes were the starting point and test bed for the efficacy of use when it comes to RPA.

Through its implementation, the Bank was able to reduce manpower hours by 30 percent, which demonstrated the advantages of deploying automation for repeatable and manual processes.

Other realised benefits include:

- reduction in error rates due to automation of manual activities,
- improved compliance and increased auditability of activities,
- reduced manual hours performed by analyst teams with valuable time savings placed in higher value work,
- standardisation of transaction monitoring processes across the Bank,
- a value-chain of "robots" where data collected through RPA can also be used in other downstream processes.

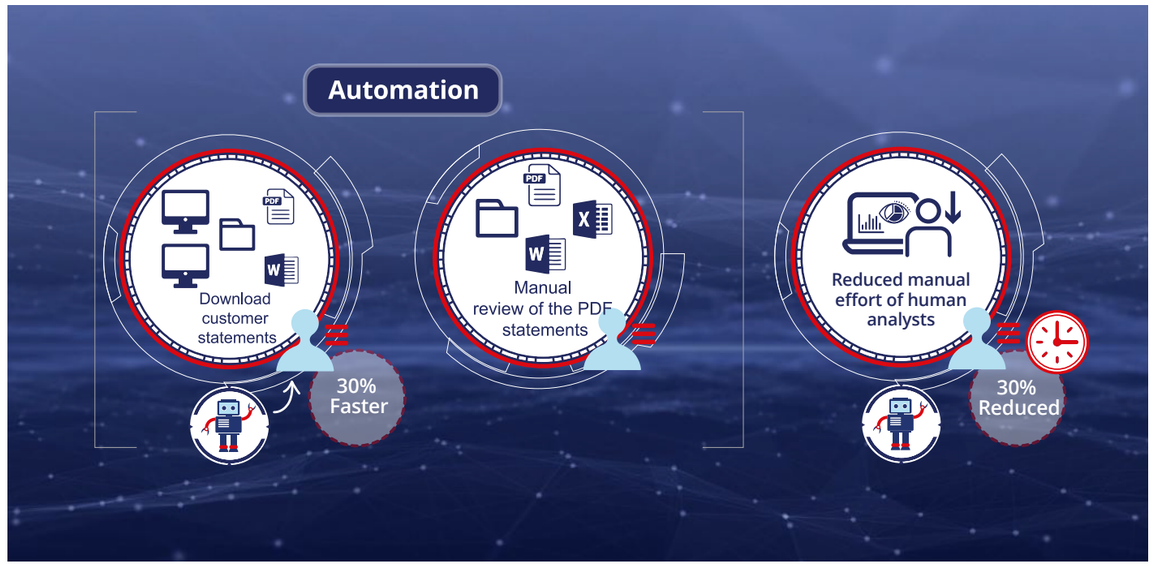
While the Bank welcomes the efficiency gained, the best outcome from RPA resides in its ability to improve oversight and operations.

In light of the aforementioned benefits, the Bank's team of analysts can afford far greater attention on suspicious alerts, maximising their investigative expertise and unique value judgement in detecting and preventing financial crime.

Over time, the value attained is a stronger risk management framework and the synergies from humans and machines working in tandem with each other. Following the Bank's proven success in using RPA within transaction monitoring, UOB will look at implementing RPA in other areas of its compliance operational framework.

With the use of RPA, the 'Triple-A approach' seeks to create continuity in the process of name screening and transactions monitoring. For instance, once the process of triaging alerts become more effective through the use of ML, the ensuing process to dispose or investigate high risk alerts is readily optimised by deploying RPA.

Figure 7: The use of RPA in UOB's 'Triple-A approach'.

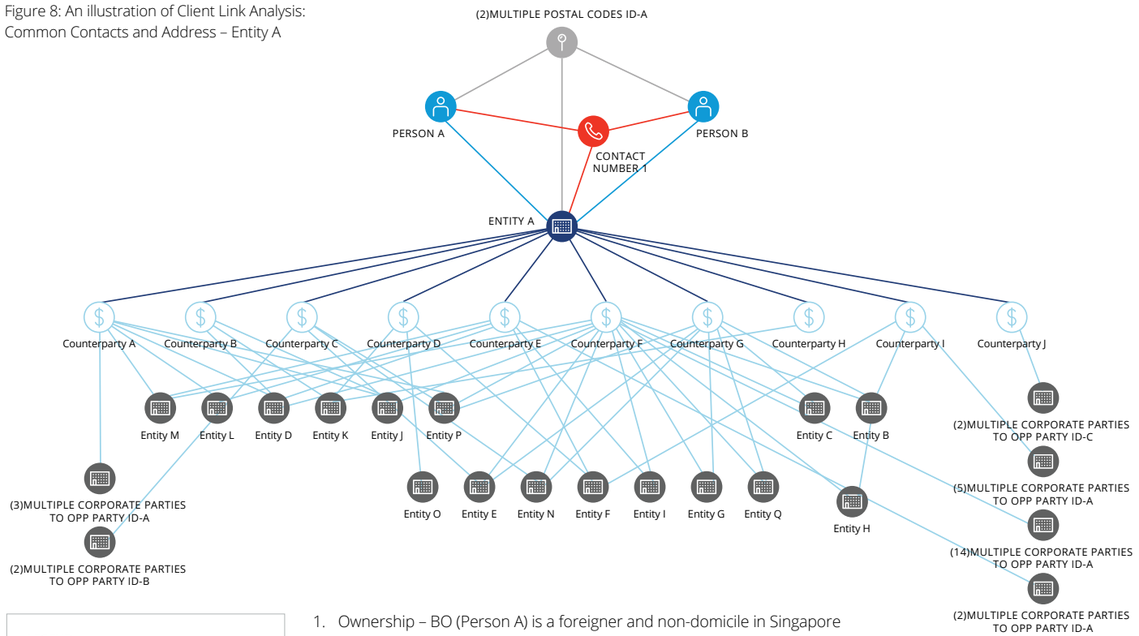


3

Pushing the boundaries of insight with Analytics

In our hyper-connected world dominated by numerous channels, systems and infrastructure, organisations faced with petabytes of information and data points need to adopt an intelligent approach towards combatting financial crime. At the heart of it, the Bank's 'Triple-A approach' combines various technologies such as advanced analytics to safeguard against financial crime challenges and provides a better response. Through an in-house developed network analysis approach, the Bank is committed to enhance its capability to analyse flow of funds to discover hidden links and anomalies, advanced schemes of layered and hidden relationships.

Figure 8: An illustration of Client Link Analysis: Common Contacts and Address – Entity A



1. Ownership – BO (Person A) is a foreigner and non-domicile in Singapore
2. KYC – Entity A is a registered address and BO address (Person A) revealed address of a corporate secretary company (Person B)
3. KYC – Shared contact details (e.g. phone, email) between Entity A BO (Person A) and Person B (corporate secretary)
4. Payments info – Company address provided by Entity A for remittances/TT instructions also bear the same address as the corporate secretary

For instance, to tackle shell companies and ultimate ownership, UOB used link analysis to evaluate and pinpoint direct and indirect relationships and trace the flow of illicit funds that carry shell company characteristics. Combining data from multiple sources (e.g transactional data, customer profile data, common contact details, and counterparty data) enabled the Bank to evaluate with greater accuracy high-risk and suspicious behaviour.

Using traditional methods that review isolated accounts could mean months of analysis to deduce incoherent relationships or unusual payments and transactions. With network link analysis, the Bank had the ability to narrow down and investigate networked relationships that carry AML and CFT risks within a few days.

With technological advancement and the increased opportunities for global commerce, organised crime syndicates continue to adapt and to evolve their techniques to exploit gaps in the global financial economy and the ubiquity of cross-border transactions. It is of paramount importance for banks to retain the ability to trace the flow of funds and identify companies set up to mask the true sources of funds and wealth. UOB's use of network analytics (See Figure 9) has enabled the Bank to identify circular, looping fund flows.

Outcomes

With network link analysis, the Bank was able to conduct faster reviews and gain more efficiencies.

This meant a reduced amount of time taken to investigate networked relationships from months to a few days.

Further, the Bank was able to ascertain some of these suspicious activities, resulting in the exit of more than 50 relationships.

Chapter 4:

Getting ready for the new world

The Future of Financial Crime Compliance | Chapter 4: Getting ready for the new world

Deciding which technologies to leverage and matching it to serve various business purposes and meeting regulatory compliance expectations is a herculean task. However, for a bank to remain competitive and resilient, it is important to employ new approaches to tackle an evolving financial crime problem.

Industry players (not just financial institutions) will need to invest in building the capacities of talent, creating sufficient players and users of AI, ML, RPA and cognitive technologies in financial crime compliance, and the infrastructure architecture of the future.

The future of financial crime compliance is certainly here, though few have stepped out with a bold proposition. The potential future-state of financial crime compliance that use of AI, ML, RPA and NLP across all processes that goes beyond transactions monitoring and name screening is being designed.

The objective is to bring about greater effectiveness and soundness in the design of financial crime compliance operating model.

A better approach to monitoring in our view has to be threat based rather than atrophying resources into monitoring everything, thereby losing focus and momentum.

An ultimate model is the rise of compliance utilities at an industry level for KYC, customer due diligence and transactions surveillance. As such, these same compliance utilities ought to be technologically enabled by next-generation technologies. In this same vein, there are compelling reasons for financial institutions to start their own innovation journey to fashion their readiness for plugging into these utilities as they move into the future.

In order to achieve this, there is a greater need today for public private partnerships to share data and insights without being hindered by the fallacy that compliance and data usurp competitive advantage.

Today, such sharing can give rise to benefits in the form of harmonised standards and analysis of threats that will not only be effective in sharpening the capability of monitoring risk, but also provide longer term gains of efficiencies.

As greater progress is made into the use of technology to ensure financial crime compliance, we will provide additional learning from UOB on their deployment of ML models, how we see the creation of the eco-system developing and the outcome of the holistic surveillance approach. We will also complement the information with our views which we hope by then, would be the target state of the future of financial crime compliance.

Banks should take a fresh approach to talent management to prepare for the future of work. Automation, the gig economy, crowdsourcing, demographic shifts all impact how work is done in the future. In the future, it is far more important to create value by problem-solving and creativity. Problem-solving skills need to command creativity, judgment, persuasion and empathy in a machine-dominated world. There needs to be accelerated learning, as with the passing on of such knowledge must be a priority.

Talent: With the future of work near, learning how to learn could be crucial, p13, *2019 Banking and Capital Markets Outlook, Deloitte*

The key areas that require immediate attention for investments into are:

Skills and expertise - as new technologies and innovation transform the nature of work, compliance officers within financial institutions will increasingly need to supervise and oversee technologies within financial crime compliance.

Creation of an eco-system – with no ready eco-system for the Bank to tap into today, we believe that the deliberate "creation" of the eco-system is needed. This is to ensure sustainability of what is starting to become an answer to the myriad of issues faced in combating financial crime. There is a need to carefully maneuver through this to avoid a "one time success wonder."

The sharing of success stories is not only essential but critical to push the envelope and entice other players to embark on the same journey. **With an eco-system, it will spur activity, strengthen capabilities, create value, and enable innovation to thrive, thereby creating a strong and evolved supply and demand of participants that will benefit the entire industry.** UOB has taken progressive steps towards contributing to the creation of the eco-system.

"Singapore is in the frontline of the digital race and the first to be disrupted are the financial institutions. With technological innovation as the new normal, the fast-paced changes have to be dealt with clear intent, motivation and decision making. Following the nation's first AI model governance framework, our team together with UOB, are set on a critical journey. The future of financial crime compliance has the potential to be seen in new light, with its seamless tie up with smart technologies, it will increasingly be a case of better insight from both a risk, as well as an opportunity angle."

Ho Kok Yong
SEA Financial Services Leader, Deloitte

End notes

1. Radish Singh, Nick Lim, Eric Ang, 'The Case for Artificial Intelligence in combating money laundering and terrorist financing', Volume 1, November 2018, Deloitte and UOB, https://www2.deloitte.com/sg/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html
2. Val Srinivas, Angus Ross, 'Accelerating digital transformation in banking', October 9, 2018, https://www2.deloitte.com/us/en/insights/industry/financial-services/digital-transformation-in-banking-global-customer-survey.html#endnote-sup-2
3. Bernardo Arnaud, 'Open banking, and what it means for European fintechs and consumers – part 1', September 12, 2019, https://www.eu-startups.com/2019/09/open-banking-and-what-it-means-for-european-fintechs-and-consumers-part-1/
4. Financial Conduct Authority, 'Global Financial Innovation Network (GFIN), August 9, 2019, https://www.fca.org.uk/firms/global-financial-innovation-network
5. Mr Tharman Shanmugaratnam, 'Banking Liberalisation's Next Chapter: Digital Banks', Keynote address by Senior Minister and Chairman, Monetary Authority of Singapore at The Association of Banks in Singapore's Annual Dinner, June 28, 2019, https://www.mas.gov.sg/news/speeches/2019/banking-liberalisations-next-chapter-digital-banks
6. DigFin, 'How UOB will position its digital bank', September 3, 2018, https://www.digfingroup.com/uob/
7. Monetary Authority of Singapore, Media Release, 'New regulatory framework to enhance payment services in Singapore', November 19, 2018, https://www.mas.gov.sg/news/media-releases/2018/new-regulatory-framework-to-enhance-payment-services-in-singapore
8. Monetary Authority of Singapore, Guidelines to MAS Notice 626 on prevention of money laundering and countering the financing of terrorism, April 24, 2015, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines-to-MAS-Notice-626--April-2015.pdf?la=en&hash=4ADAD30E6B7E97D4E67B3650AFC90F72639C2571
9. Personal Data Protection Commission, Singapore, 'A proposed model AI governance framework', first edition, January, 2019, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Model-AI-Framework---First-Edition.pdf
10. Singapore Business Review, 'Tookitaki Holding takes home AI Award for banking at SBR's inaugural Technology Excellence Awards', 31 May 2019, https://sbr.com.sg/co-written-partner/more-news/tookitaki-holding-takes-home-ai-award-banking-sbrs-inaugural-technology
11. World Economic Forum, Technology Pioneers 2019, https://widgets.weforum.org/techpioneers-2019/companies/tookitaki/

Contact us

Radish Singh
Southeast Asia Financial Crime Compliance Leader and AML Partner, Deloitte Financial Advisory, Forensic, Deloitte
radishsingh@deloitte.com

Min Liu
Associate Director
Deloitte Financial Advisory, Forensic, Deloitte
jiamliu@deloitte.com

Nick Lim
Head of AI, Analytics & Automation Group Compliance,
United Overseas Bank
Nick.LimYC@UOBgroup.com

Eric Ang
Head of Compliance Analytics & Insights, Group Compliance
United Overseas Bank
Ang.BoonHin@UOBgroup.com

Deloitte.