



Advanced analytics and
innovation in Financial
Crime Compliance
The future is now

Glossary of terms

AI	Artificial Intelligence
AML	Anti-Money Laundering
BAU	Business as Usual
CFT	Countering the Financing of Terrorism
DMO	Data Management Office
FCC	Financial Crime Compliance
FEAT	Fairness, Ethics, Accountability and Transparency
FI	Financial Institution
GC	Group Compliance
MAS	Monetary Authority of Singapore
ML	Machine Learning
NLP	Natural Language Processing
NS	Name Screening
POC	Proof of Concept
RPA	Robotics Process Automation
TM	Transaction Monitoring

Foreword



This third white paper, co-published by Deloitte and UOB, examines the use of innovation and advanced analytics in a world dominated by digital technology and disruption. We will touch on potential risks that stem from business disruptions in unprecedented times, including how the global coronavirus pandemic has resulted in a rise in financial crime. We describe how technology and innovation are necessary in weathering unforeseen circumstances and in achieving better outcomes for Financial Crime Compliance (FCC).

The financial services sector is now facing greater challenges from sophisticated criminals who have found ways to profit from an increasingly digitalised economy, accelerated partly due to the COVID-19 pandemic. Efforts to enhance detection by augmenting investments made in artificial intelligence (AI) and machine learning (ML), analytics and robotic process automation (RPA) have paid off. However, more work still needs to be done to ensure that the sector is able to adequately respond and curb various risks including financial crime, and maintain the trust it has established with its relevant stakeholders.

Our white paper examines the ongoing journey of UOB's AI anti-money laundering solution, from proof of concept (POC) to production stage, explaining how it gradually calibrated models for integration into current banking operations. It outlines the justification for the Bank's investment in advanced analytics, AI/ML and robotics – noting how these have been instrumental in mitigating major disruptions.

Deloitte and UOB previously published two white papers in 2018 and 2019. The first white paper titled, "The case for artificial intelligence in combating money laundering and terrorist financing"¹ explains how financial institutions (FI) can leverage innovation to manage FCC effectively. It shared UOB's case study in successfully piloting machine learning to identify suspicious accounts and transactions with greater accuracy. The second white paper titled, "The future of financial crime compliance"², depicted the future-state of FCC that incorporates AI, ML, RPA and natural language processing (NLP) to manage evolving financial crime risks. It details what is involved to operationalise ML for FCC, taking reference from UOB's successfully implemented ML model.

Sharing UOB's transformation story – on its use of innovative technologies to combat financial crime provides insight into the implementation process and challenges experienced. It sheds light on the governance of the technology, the engagement required with stakeholders to build trust in the solutions, and how to integrate these into the business as usual operating environment. We hope the insights shared in this white paper will encourage FIs to focus on applying FCC technologies, reaping its benefits, while helping to innovate in and enhance FCC efforts across the industry.



Introduction

The global pandemic, as well as geo-political tensions and looming trade wars dominated the headlines in 2019 and 2020 representing a new global reality marked by disruptive events. COVID-19 has prompted governments from all countries to take drastic measures³ from lockdowns to enforced business closures. Traditional businesses have been hit hard by these measures, especially where operations remain brick-and-mortar-based.

In response, businesses and Financial Institutions (FIs) have accelerated investments in transforming their business models, and embracing digitisation and enhancing remote working capability. While this move to digitisation has helped to lessen the impact of COVID-19 disruption, according to a Financial Action Task Force (FATF) publication in May 2020⁴, it has also brought new challenges and heightened concerns in dealing with new and varied forms of financial crimes.

Widening sophistication in crimes such as fraud, cybercrime, human trafficking, slavery, crimes against the environment, online child exploitation and organised property crime necessitates even greater efforts to combat financial crimes. There is therefore an urgent need for the industry to explore and to apply innovative technological solutions that can address these complexities and risks. We hope this paper inspires the industry to embark on this journey and to build a more robust financial crime risk management ecosystem.

The need to innovate and to adopt technology has never been more pronounced. Technology and digitisation are no longer a “good to have” for businesses. Businesses need to stay connected, and overcome constraints of physical mobility with the help of technology. Agility is highly priced. This has a direct effect on FCC where embracing innovation with use of AI and ML and cutting-edge technology will enhance capability, effectiveness and efficiency in combating financial crimes.

Anna Celner
Deloitte Global Banking & Capital Markets Practice Leader

How can FIs embrace this new reality of innovation?



In 2020, worldwide revenues for AI/ML companies are expected to exceed USD 150 billion, representing a 12.9% increase from 2019⁵. The banking industry invested a total of USD 5.6 billion in AI-enabled solutions in 2019. According to a study, companies see AI and ML as important components in their strategy where significant investments have been and will be made. Risk management has also been highlighted as the top domain for AI/ML implementation.⁶

The increase in AI/ML investment underpins the increasing dependence by businesses on technology to manage enterprise-wide risk. This chapter examines the various investments made into technologies such as AI/ML and data analytics, and how this has been a game changer for FIs in managing financial crime risks.

Effectiveness and efficiencies of advanced analytics

As more people go online, data is becoming plentiful and pervasive. FIs and organisations have been analysing data to understand transaction behaviours and spending patterns. They are also designing new products and services to meet changing customer needs. For example, Singapore-headquartered bank UOB has used insights from transaction data to personalise the banking experience for consumer and business customers across its network in Asia.

In the FCC space, data has also been used extensively in identifying bad actors who try to use FIs as conduits to launder illicit funds. Typically, such surveillance includes identifying complex money laundering typologies, anomalous transactions and suspicious fund flow networks.

The positive impact of data analytics on FCC has been immense. For instance, it was reported that an analytics solution applied by a FI uplifted its capabilities to detect and to deter fraudulent attempts. This resulted in a 26 per cent increase in suspicious cases investigated and a 40 per cent increase in submission of proven fraud cases for criminal prosecution. Collectively, this translated to a substantial recovery of money lost from fraud for the FI.⁷

Swift detection of suspicious human behaviour

AI/ML has also been a topic of interest as FIs commit hefty budgets to managing risks more efficiently and effectively. Our first white paper discussed the application of ML algorithms with self-learning capabilities that enable FIs to plough through large volumes of data for potentially suspicious customer transaction behaviours. Implementation of such platforms enables FIs to direct resources to tackle fraud alerts that are likely to be true, reducing time and effort on false positives. This places FIs in a good position to address more fraud incidents without a significant increase in manpower. Furthermore, accurate and swifter identification of fraud facilitates a faster recovery of funds lost.

For example, a bank in Indonesia uses ML to detect new suspected fraud patterns. The implementation of this platform has reaped significant results with a 30 per cent reduction in the number of fraud incidents due to more accurate detection.⁸



Adaptability in changing circumstances

As AI/ML models can adapt to changing FCC patterns over time, they offer significant benefits in the current disruptive environment.⁹ The adaptive learning capabilities of AI/ML are sometimes overlooked and undervalued when benefits of this attribute are not apparent in the initial stage of investments made into these technologies. Some organisations may see these as new technologies, and question if they can be dependable and defensible under intense scrutiny.

Yet, traditional systems are not the best when it comes to agility. Despite the effectiveness of rule-based systems in detecting transaction anomalies, ever-changing customer behaviours and transaction patterns mean these systems have to be constantly re-calibrated. This is a highly manual exercise.

That is why many organisations are moving towards models that adapt to the changing environment and self-learn to provide insights that can be acted on by compliance officers. Shifting from the limitations of traditional rule-based systems to learning-based ML models, can help FIs vastly improve accuracy in detecting and deterring potential financial crimes.

Automating repetitive jobs

In our previous white paper, we delved into Robotic Process Automation (RPA). We highlighted the key benefits of automation and how it is now a “must-have” for FIs to achieve scale and value more efficiently. The automation of repetitive and low-value activities ensures that human resources are deployed efficiently and higher value activities receive more attention. This way, human expertise can be maximised to combat financial crime.

UOB, with Deloitte's assistance, successfully implemented RPA in transaction monitoring. With robots taking on manual and repetitive processes, this has led to a decrease in human error and an improvement in the standardisation of transaction monitoring processes and auditing of activities. The Bank was hence able to achieve a reduction of 30 per cent in man-hours spent on these manual processes. Typically, these tasks would have been cumbersome to perform in remote working circumstances during the pandemic. The use of RPA has enabled the efficient performance of these tasks without disruption.

Progress will result in more benefits

COVID-19 has necessitated the urgent adoption of technology and digitisation to continue business-as-usual (BAU) operations, with remote working now the global norm. Our findings also demonstrate that investing in innovation and technology helps keep FIs ahead in these volatile times.

Investments into technologies for FCC will be critical for FIs to keep abreast of evolving financial crime threats. FIs that have been digitalising their services would have seen some returns on investments amid the tumultuous times, as they were able to avoid a complete standstill of operations. Beyond this, FIs also need new approaches and advanced data and technology capabilities to continue efforts to become more robust and effective in managing financial crime risks.

Ho Kok Yong
Deloitte Southeast Asia Financial Services Industry Leader

With the competition from financial technology (FinTech) firms, established FIs cannot afford to rest on their laurels. FIs have to innovate continuously to avoid the erosion of their business advantage. They also need to devise market-friendly cost structures, facilitate transactions with minimal friction and safeguard revenues. Innovation is not only relevant to business (front-line) but also in compliance and more particularly, in FCC. As FIs innovate and compete from business perspective, compliance generally and FCC need to keep pace to continue to be effective. For instance, as funds move faster across borders, trade transactions become more complex, customer behaviour change rapidly and criminals conjure-up new approaches to launder money through FIs, the capability for surveillance and detection of financial crime must also become equally robust. This can be achieved with the use of AI, ML and RPA.

Investments into innovation and technology also cannot be a one-off occurrence. Constant refinements to keep technology current are essential in managing ever changing financial crime risks and regulatory expectations. This calls for the development and implementation of more sustainable and adaptive technologies such as ML. These are self-learning and can automatically calibrate as the patterns of financial crimes advance.

As highlighted in the previous white papers, employees also need to be trained to be proficient users of the output of data analytics, AI/ML and RPA. This will ensure they are capable of supervising and operating FCC technologies.

The trajectory to achieve the end-goal

Continual investment into AI/ML to combat FCC is required to address the increased dimension of financial crime risks devised by increasingly sophisticated criminals. It is also crucial for FIs to ensure that they quickly develop these innovations to strengthen their risk management capabilities and to stay ahead of the criminals.

As previously mentioned, AI/ML models used for FCC enable FIs to strengthen surveillance against financial crime. These tools enhance the FIs' abilities to identify anomalies, so as to mitigate money laundering and terrorist financing risks.

Current landscape

The use of advanced analytics and innovative technologies for FCC is still in its infancy. What is clear is that management buy-in is required before any FCC approach can be transformed with new technologies. Given new technologies require initial financial investments before efficiencies and effectiveness for FCC can be demonstrated and realised, faith is needed that these new technologies will work. Convincing stakeholders can be a challenge, and investments to support development are sometimes made in tranches as the technology's success is realised step by step.

For AI/ML solutions to be defensible, development timelines may also be extended. This is to avoid risks and regulatory implications, should these AI/ML models fail.

The end-goal

For AI/ML models to deliver their maximum potential for FCC, all parties (FIs, employees, service providers and regulators) will need to have trust in them. This level of trust in models has to be the end-goal for the industry, or it will impede development.

Providing a secure banking environment deepens consumer trust and confidence in the financial system. Ultimately, FIs rely on trust from their customers to build a sustainable business. In that light, they must preserve stakeholder value and support from governments and institutional investors, among others.

Bridging the trust gap

Any breakthroughs in the use of AI and ML for FCC would be undervalued without trust in the technology solution from stakeholders. In addition, regulators also need to trust the decision process to embrace innovation and solutions being assured that these models are explainable, defensible and can address FCC risks effectively.

Appropriate perimeters and rubrics need to be created to prove the effectiveness of AI/ML models as a trusted ally for humans in tackling FCC issues. This point was reiterated at the G20 Digital Economy Ministers Meeting by Singapore's Minister for Communications and Information, S Iswaran. He highlighted the paramount importance of upholding trust and security in the deployment of AI and data flow in an increasingly digitalised world¹⁰.

To address this requirement, many have either established or suggested tangible frameworks and guidance for such AI models. For instance, the European Commission¹¹ published a white paper on AI that emphasises focusing on trustworthiness in the usage of AI/ML as it sets out policy frameworks to ensure a greater uptake of AI/ML. This rings true in the United States as well, where the White House Office of Science and Technology Policy¹² provided government agencies with guidelines and principles for "considering regulations or policies related to AI applications". Public trust and disclosure, and transparency are listed as key principles.

The Institute of International Finance (IIF) and Deloitte have also, in October 2019, released a white paper calling for a combination of regulatory reform, cultural change and the deployment of new technologies to enhance how FIs counter anti-money laundering (AML) threats.¹³ Engaging key stakeholders in various stages of the development process of innovative solutions is a necessary step – it bridges the trust gap and builds confidence in the use of such technology for combating financial crime.

The Monetary Authority of Singapore (MAS) has also published a set of principles to promote fairness, ethics, accountability and transparency (FEAT). These are intended as "an industry benchmark and guide when thinking about how to use AI and data analytics"¹⁴. The FEAT principles can also help strengthen internal governance of AI applications as well as build greater trust and confidence in AI/ML solutions.

In October 2019, the Institute of International Finance (IIF) and Deloitte published a whitepaper calling for a combination of regulatory reform, cultural change, and the deployment of new technologies to better counter threats posed by illicit money flows through the international financial system. Innovation, with the use of AI/ML and RPA, is a necessary step towards bridging the gap and becoming more effective in combating financial crime and building trust. In addition, as discussed in the Deloitte / IIF whitepaper, recommendations such as public-private partnerships, improving information sharing, and reforming suspicious activity reporting are all necessities in sharpening capabilities to combat emerging financial crime threats.

Michael Shepard
Deloitte Global Financial Crime Practice Leader



To provide a set of guidelines against which FIs can validate their success, the MAS brought together a consortium¹⁵ consisting of FIs and FinTechs, of which UOB is a founding member. Its aim is to create a framework known as “Veritas” to provide FIs with a verifiable way to incorporate the FEAT principles into their artificial intelligence and data analytics (AIDA) solutions. While still in the early stages of development, this framework seeks to “promote the responsible adoption of AIDA”¹⁶. In a similar vein, Deloitte has envisaged that “Trust and Confidence” should form the foundation on which all AI/ML models are built. The company has been a big advocate in building trust between man and machine to work towards a common set of goals since the first white paper published with UOB on AI/ML in FCC in 2018.

Industry players such as Microsoft¹⁷ and the Gartner Group¹⁸ have also proposed the use of frameworks with a focus on using maturity models to bolster confidence and to catalyse greater adoption of AI/ML. Maturity models are frameworks that help industry players measure their readiness and potential (i.e. their current and future state) to implement AI/ML.

Specifically, parties involved should be:

- 1) provided with the means to measure the maturity of FCC AI/ML models; and
- 2) able to identify and implement adequate governance and risk management around specific models.

There is therefore a need to harmonise AML/CFT requirements and the principles governing AI/ML to build an adequate framework for FCC operations. In the FCC space, Deloitte views collaboration in the form of public-private partnerships (PPP) as central to improving the “legal and regulatory framework and risk management toolkit to enhance effectiveness”¹⁹.

Given that such technologies are quickly becoming embedded within FCC programmes, the industry should deepen collaboration and accelerate the building of these capabilities to bolster trust and build an ecosystem. The next step, is to create industry-level monitoring utilities incorporating AI and ML, amongst others. With the use of AI / ML and other innovation, as FIs become more effective at managing financial crime risks, the industry could together embark towards a greater win-win phenomenon to combat financial crime more effectively.

Radish Singh
Deloitte Southeast Asia Financial Crime Compliance Leader



Measuring maturity

We take the view that the development of a maturity model will provide an industry-wide yardstick for use of AI/ML models in FCC. Currently, no industry benchmarks exist to measure and test the maturity of the framework for deployment of advanced analytics and innovation. There are also other obstacles:

- 1) **Protracted development timeframe:** Various FIs have collaborated with regulatory technology (RegTech) companies, for example, UOB and Tookitaki. Custom-built models can be co-created in such collaborations to fit an FI's specific requirements and architecture. In the absence of an industry maturity benchmark, FIs and their vendors have to define an ideal state and to chart their own course in terms of addressing gaps in or measuring the efficacy and robustness of their models and the governance framework. Unsurprisingly, this exercise lengthens the production timeline and is subject to much challenge due to the lack of a benchmark framework for comparison.
- 2) **Inadequate user reliance:** FIs who have been identifying gaps during the development process, may be reluctant to trust the model, especially in the absence of an objective benchmark to evaluate its maturity.
- 3) **Duplicate operations:** The lack of regulatory guidance has resulted in FIs being reluctant to rely entirely on AI/ML models. FIs use both AI/ML models and traditional FCC methods to tackle the same alerts, resulting in duplicate work.
- 4) **Regulatory scrutiny:** Regulators may increase scrutiny on a FI to ensure the AI and ML model's efficacy as it is adapted for use in FCC. The model needs to be explainable and robust in managing financial crime risks. There is zero tolerance for failure given that the stakes are too high for any financial crime to pass through an FI. However, literature providing clear regulatory guidelines specific to FCC-related AI and ML systems is currently unavailable.
- 5) **Inadequate internal governance principles and guidelines for assurance framework:** As with any models deployed and processes put in place to manage risks, there is a need for a governance and assurance / testing framework. Deloitte and UOB have brought together various principles and standards based on our experience while working together on this journey. These include best practices and international regulatory principles which could be applied by analogy, given that there are no existing direct guidance for reference. We created documentation on governance and model risk management principles as well as processes to address lower value alerts with due consideration.

Closing the maturity measurement gap

A potential maturity model for use of AI/ML in FCC, as discussed above, can help the industry better assure stakeholders that the AI/ML solutions are robust for use. Specifically, the following are required:









- 1) **Providing a standard measure of maturity:** The industry should be able to gauge the models' capabilities and maturity in a way that enables them to discern competent models from those that require further improvement. This in turn allows them to operate fit-for-purpose systems with assurance (in the case of FIs and employees) and withstand any heightened scrutiny on their operations (in the case of regulators). A maturity model will also aid in setting standards to manage and mitigate model subjectivity and bias. It also facilitates the interoperability of champion and challenger models to continually ensure fitness of purpose. In addition, there should also be guidelines to define the acceptable industry approach to governance and ongoing assurance.
- 2) **Shortening development timelines:** Using the said yardstick, FIs and their partners would have a reference point for their development and implementation roadmap and can more quickly identify and address gaps within their AI/ML models for FCC.
- 3) **Facilitating strategic decision-making:** In the longer term, FIs will be able to properly position their current situation in terms of organisational maturity as well as make strategic decisions with visibility on future AI/ML models according to a development roadmap. We are hopeful that in the near future, there will also be further guidance on the use of algorithms in managing financial crime risks.
- 4) **Better training and awareness:** With an industry yardstick, this reference point will also help to guide stakeholders' understanding of such models.

Characteristics of a maturity model

Based on the journey of Deloitte and UOB as well as work and research undertaken in this space, maturity models have two key components:

- 1) **Staging Mechanism:** Roadmap setting out the stages of an organisation's AI maturity – ranging from aspirational to advanced implementations.
- 2) **Guiding Principles:** A set of principles underpinning development and operationalisation. These principles can be summarised into four large categories: i) Culture; ii) Governance and Training; iii) Data; and iv) Model Architecture.

A maturity model for the use of AI/ML must be tailored to address specific needs in FCC. Even though the current general maturity models in their present forms are inadequate for FCC purposes, they can provide a baseline to start with when designing a bespoke model to account for the peculiarities of financial crime-related risks and issues. Added considerations include:

- | | |
|---|---|
|  Compliance with regulatory requirements |  The explainability of models and algorithms |
|  Establishing culture principles such as "Tone from the Top" |  Designation of roles and responsibilities (across Three Lines of Defence) |
|  Undertaking a risk-based approach |  Maintaining documentation and an audit trail |
|  Putting in place clear policies and procedures for governance, risk management and escalation |  Adequate training and awareness for staff |

A scoring matrix can be used to highlight where FIs are performing well and where there is a need for improvement. A staging framework should also be constructed to provide the direction for future FCC-related AI/ML models.

Appended is a suggested maturity model framework based on Deloitte's experience thus far. We believe this forms the starting point for developing a maturity model that we can be refined and enhanced alongside developments in AI/ML for FCC.

Deloitte's suggested FCC maturity model

Figure 1 outlines our suggested guiding principles incorporating key FCC requirements.

Figure 1: Guiding Principles

 <p>Culture</p> <p>Tone From the Top Encouraging responsible use of AI to enhance compliance capabilities and cultivate an innovative culture</p> <p>Data-Based Decision Making Strategic decisions made by the FI are driven by data analysis in reliance on the model</p> <p>Risk Based Approach / Effective Cascade of Risk Appetite Adopting RBA as encouraged by regulators, calibrating model to risk appetite of FI set by senior management where relevant (e.g. How alerts are triaged)</p>	 <p>Data</p> <p>Standardisation of Data Data should be uniform across the FI without overlap</p> <p>Adequacy of Data Pools / Lakes Data used should be adequate and sufficient for the model's purposes</p> <p>Customer Identification Entity resolution abilities of models must be adequate for purposes of accurately identifying individual customers</p> <p>Quality Management Health checks on data quality should be conducted periodically and consistently</p> <p>Privacy Customers' privacy should be kept in line with FIs' internal privacy requirements and regulatory requirements</p> <p>Data Aggregation From Business Functions Data owned by various business functions in the FI should be aggregated into a central repository / pool to facilitate oversight</p>	 <p>Governance & Model Risk Management</p> <p>Model Risk Management Monitoring of model design and conceptual soundness should be ongoing</p> <p>Model Governance Adequate and sufficient monitoring of governance (controls) should be established</p> <p>Risk Profiling & Management Model should be able to conduct risk profiling in various areas for better understanding and management of risk exposure</p> <p>Adequate Oversight Senior Management should be aware of the key risks as well as make decisions around them</p> <p>Policies & Procedures Implementation of clear processes approved by senior management for the escalation of alerts and suspicious activity</p> <p>Roles & Responsibilities Risk ownership and segregation of duties to appropriate people, assigning of responsibility for the model (E.g. Post mortem reviews: continuous gap checking to ensure if there are gaps)</p> <p>Documentation & Audit Trail FIs' customer records should be retained on file per FCC regulatory requirements of at least 5 years</p>
---	---	---



Model Architecture

Integration into BAU Operations

Model should be designed for smooth and adequate integration into BAU operations

Efficiency

Model generates alerts with greater accuracy, significantly increasing true hits and reducing false positives

Explainability

Stakeholders must be able to understand decision paths, model should be able to output clear decision paths (No black box)

Ongoing Monitoring

A periodic review of model performance metrics should be conducted to monitor performance and model health - conditions triggering re-developments and re-validations should be pre-defined



Assurance

External Validation

Model should be sufficiently validated by independent third parties such as Deloitte

Internal Validation

Internal validation conducted within the FI should aspire towards an automated self-validation module conducted solely by the model

Model Effectiveness

Model effectiveness should be constantly monitored via parallel runs, challenger models and below-line models



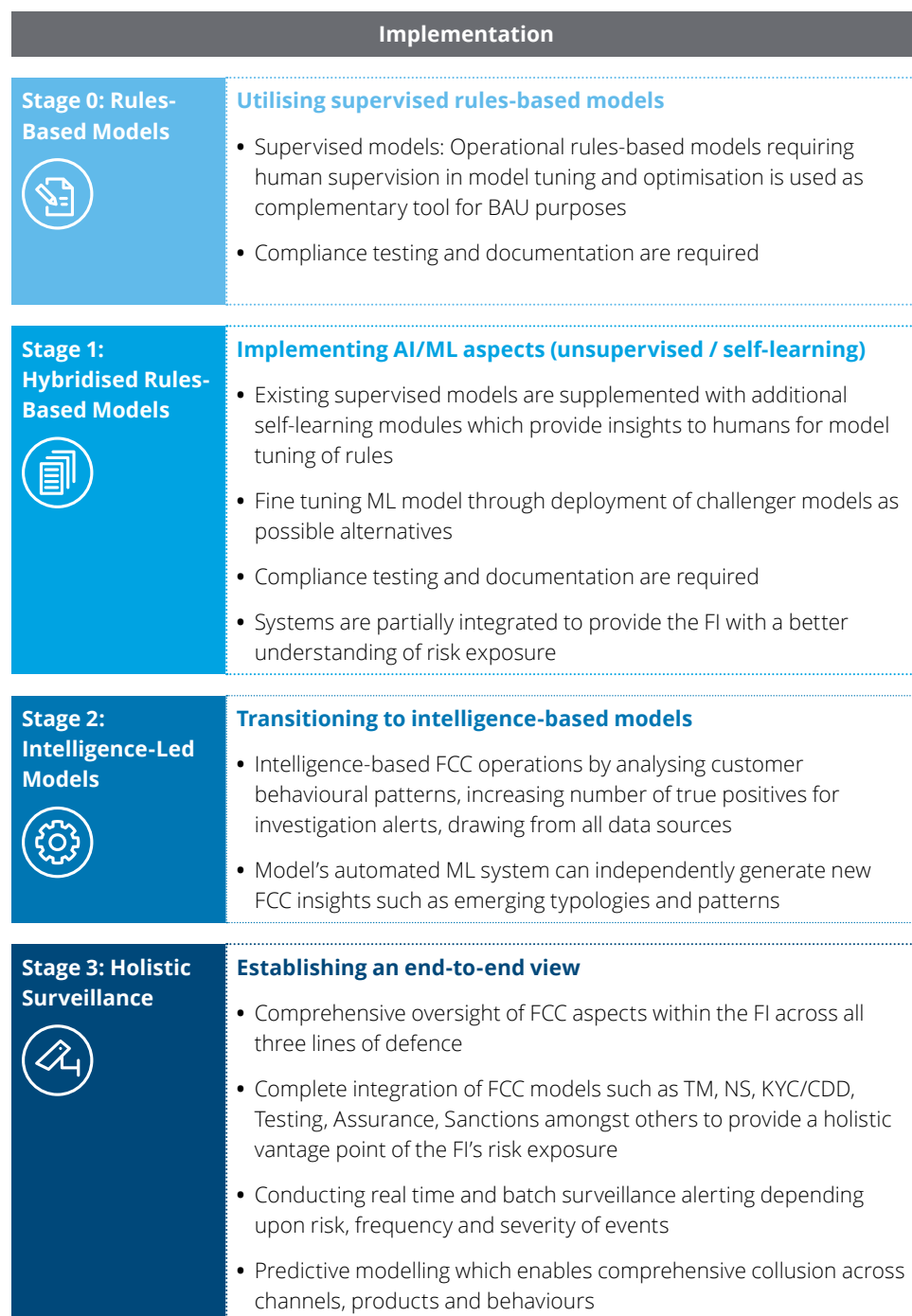
Training

Human Resource & Training

Ongoing training to ensure proficiency in operating model / expertise as well as recruitment of relevant Subject Matter Experts in both Data Analytics & FCC

Figure 2 illustrates Deloitte's suggested FCC maturity model which builds on the above principles and incorporates a staging mechanism. Deloitte is of the view that maturity can be adequately measured by assessing a model against a scoring matrix aligned with the principles above.

Figure 2: Suggested FCC maturity model



Internal Assurance

Internal Audit by Current Teams

- Internal assurance conducted by FIs' own audit teams per current practices
- Silo-ed view of risk exposure based on scope of audit conducted

Stage 0:
Traditional
FCC 3rd Line
Assurance

**Transitioning to a supervised self-validation model**

- Self-validation module is developed running parallel with traditional internal assurance practices
- Human intervention is required to verify output and results from the system

Stage 1:
Hybridised
Assurance

**Moving towards automated self-validation**

- Self-validation module is developed in tandem with the intelligence-led model
- The model is able to conduct internal assurance independently without human intervention

Stage 2:
Intelligence-Led
Assurance

**Establishing an end-to-end view**

- End-to-end view of FIs' current FCC assurance programme using dashboards and visualisations of risks to highlight the areas requiring attention by the FIs
- An integrated view risks allows senior management to achieve better oversight leading to more informed decision making

**Stage 3: Holistic
Assurance**





Governance and risk management

Going down traditional routes

Aside from advocating an industry-wide maturity model, another approach to building trust in stakeholders is to ensure that robust governance and risk management structures are embedded within the framework when deploying AI/ML models.

Regulators have continued to stress FIs to ensure that compliance-related issues are layered with strong governance and risk management. This has been a prominent facet of financial crime compliance and will undoubtedly carry through to AI/ML models.

What to look out for?

At the core of the issue, all models need to be explainable – so that humans, especially end-users, understand the underlying logic that drives the decision-making process. An AI/ML model also needs to include adequate oversight and risk management, clear policies and procedures for escalation, designation of roles and responsibilities and model explainability.

The maturity model proposed above, aligned with the said principles, can partially address concerns surrounding governance and explainability of the model. But with the lack of uniformity in approach of AI/ML uptake in FCC, the industry can only provide a set of generic guidelines. FIs will need to adapt frameworks according to their wider governance structure, technology architecture and specific needs.

Deloitte and UOB recognised these considerations when implementing the Bank's alert triage. We developed the low priority (L1) alert management guidelines. To make AI/ML models reliable and robust, "confirmed" false positives are segregated as low priority (otherwise known as the 'L1 bucket'). Both UOB and Deloitte have developed guidelines on how to manage such L1 alerts. We have also co-created governance principles, regulatory expectations and compliance requirements.

Use case: Low priority (L1) alert management guidelines

L1 alerts hold a higher probability of being false positives. UOB and Deloitte have developed a streamlined approach to working with L1 alerts. First, the transaction alerts monitoring team analyses the L1 alerts to rule out any probability of true positives being erroneously embedded in the L1 bucket. These alerts are then filtered by mapping them against risk indicators set out in UOB's internal policies and FCC risk governance principles. The guidelines also establish prudent operating procedures for the team in the event any L1 alert is identified to have potential risks or previous linkage to STRs.

Model risk management guidelines for the use of AI/ML in FCC

One of the many principles provided in this document include the need for ongoing calibration to ensure that the model continues operating as intended.

Deloitte and UOB developed and implemented guidelines to ensure visibility of the model by applying traditional AML/CFT requirements as well as MAS' suggested FEAT principles. The guidelines cover the following, amongst others:

- a) Policies and procedures
- b) Oversight from senior management
- c) Explainability of the model's decision paths
- d) Managing bias
- e) Applying model governance principles based on international practice
- f) Assurance guiding fundamental considerations

Embedding these principles into a model with tangible and concrete steps ensures compliance as well as effectiveness of the model. With these in place, trust can be strengthened as all parties involved are able to understand the Bank's approach to managing risk even when employing non-traditional tools.

Building trust and confidence

While some FIs have been eager to implement AI/ML solutions into their FCC operations, other stakeholders have been slower to do so. These stakeholders are not opposed to deploying the use of AI/ML in FCC but are wary of the consequences, should these models fail to meet their objectives. The implications are heightened when an AI/ML model fails in identifying instances of malfeasance by a FI, its employees or customers.

UOB and Deloitte have published this series of white papers with the aspiration that other industry players can take reference from cited reliable use cases and embark on similar journeys.

Our suggested approach to constructing tangible frameworks and benchmarks for the measurement of maturity affords:

- FIs better visibility in terms of next steps
- Other stakeholders the ability to rate models and decide how much trust to place in them

Establishing good governance and risk management, and demonstrating that they have been carefully considered and implemented, will go far in bolstering regulators' confidence in a specific AI/ML model. Should these areas be achieved, the industry will be significantly closer to the desired end-state of having all stakeholders (e.g. FIs, employees, regulators) place their trust in these technologies for the purposes of FCC. This will accelerate the use of AI/ML in the industry.

UOB and Deloitte have published this series of white papers with the aspiration that other industry players can take reference from cited reliable use cases and embark on similar journeys.

Challenges

There are also other factors for consideration when implementing such a framework:

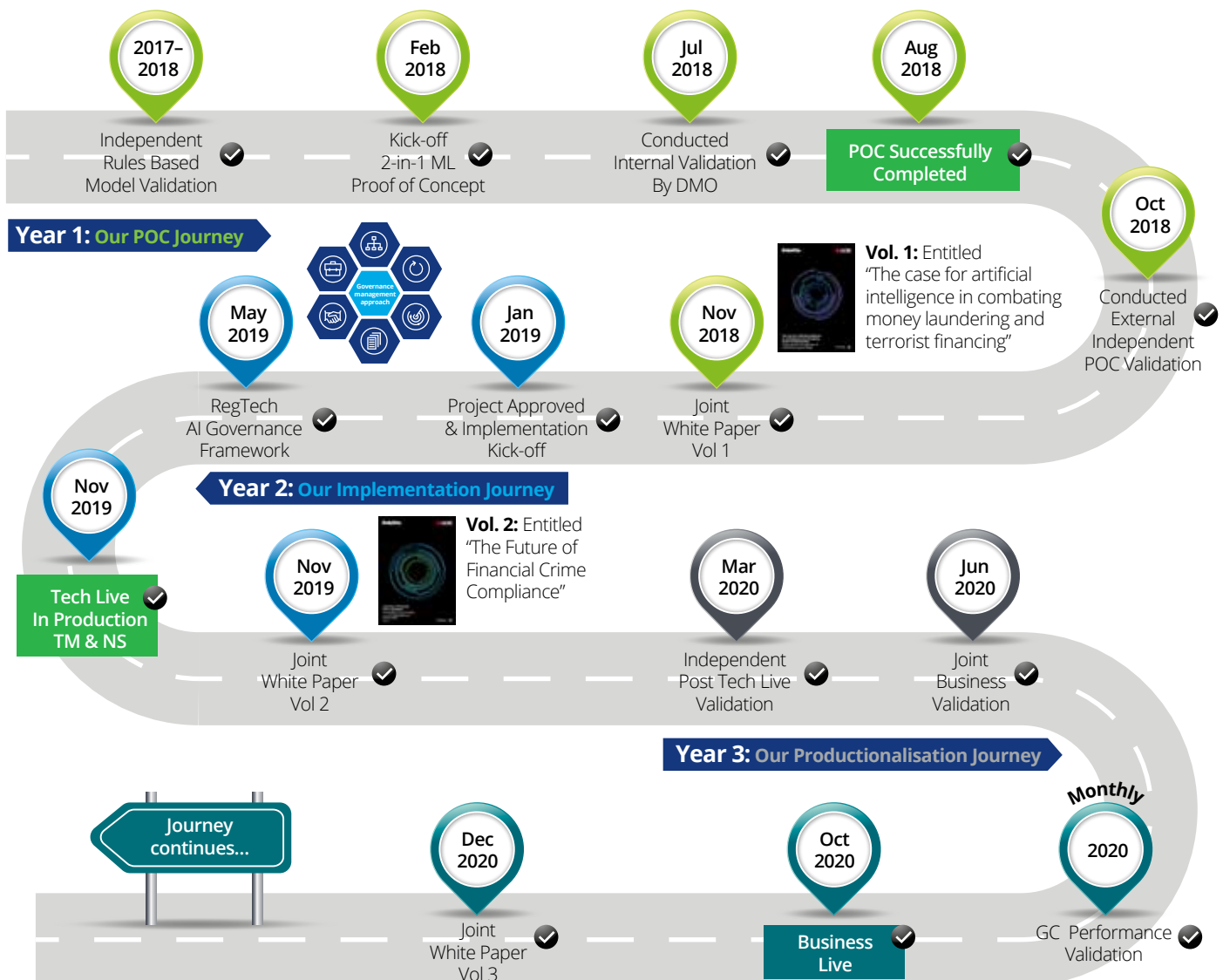
- 1) **Harmonising regulatory compliance and internal controls** – Importing regulations built for traditional FCC operations into a completely new territory of use for AI/ML in FCC requires significant work in harmonising the requirements of compliance and controls. This is necessary to manage risk alongside good governance and accountability. We sought to highlight these core principles throughout the series of white papers created by UOB with Deloitte. This journey is a continuous one as models become increasingly advanced and sophisticated, and principles need to evolve. It is not a one-off investment.
- 2) **Multiple stakeholders** – Formulating a best practice framework requires input from an entire industry and presents significant logistical challenges. The preferences of different players add to the complexity and lack of homogeneity. While it is unlikely that there will be great disagreement in terms of the broader principles and components, there could be some differences as details are worked out across the industry. The broad principles can serve as the universally applicable baseline. Each FI could then work in the requisite details based on their unique architecture and needs.

UOB's approach to developing a RegTech ecosystem

UOB's journey

Our previous white papers touched on the Bank's journey with Deloitte and RegTech firm, Tookitaki, from POC to the technical-live stage of the model. UOB and Deloitte have since made significant progress by conducting validation exercises of the production models to go business-live in the second half of 2020. This includes an independent technical-live validation conducted by Deloitte, an internal joint business validation and periodic internal performance monitoring.

Figure 3: UOB AI Journey - A prudent approach to developing a RegTech ecosystem



Conducting independent model validations - Deloitte

As discussed in our first white paper, the POC AI/ML model underwent a two-fold validation – first by UOB's data scientists within the Bank's Data Management Office and next, by Deloitte. It proves that the POC model is conceptually sound and capable of delivering good model performance.

Recognising that this AI/ML RegTech solution could play a strategic role in enhancing the Bank's effectiveness in AML risk management, UOB and Deloitte initiated additional independent assessment and validation of these models prior to going business-live. UOB also worked with Deloitte to develop a RegTech-specific AI/ML model management framework to guide key aspects of the AI governance and model architecture. This in turn ensured the model's veracity and stability.

Governance AI model management framework

In Volume 2, we laid out a model governance framework to guide the implementation of ML models in the following areas:

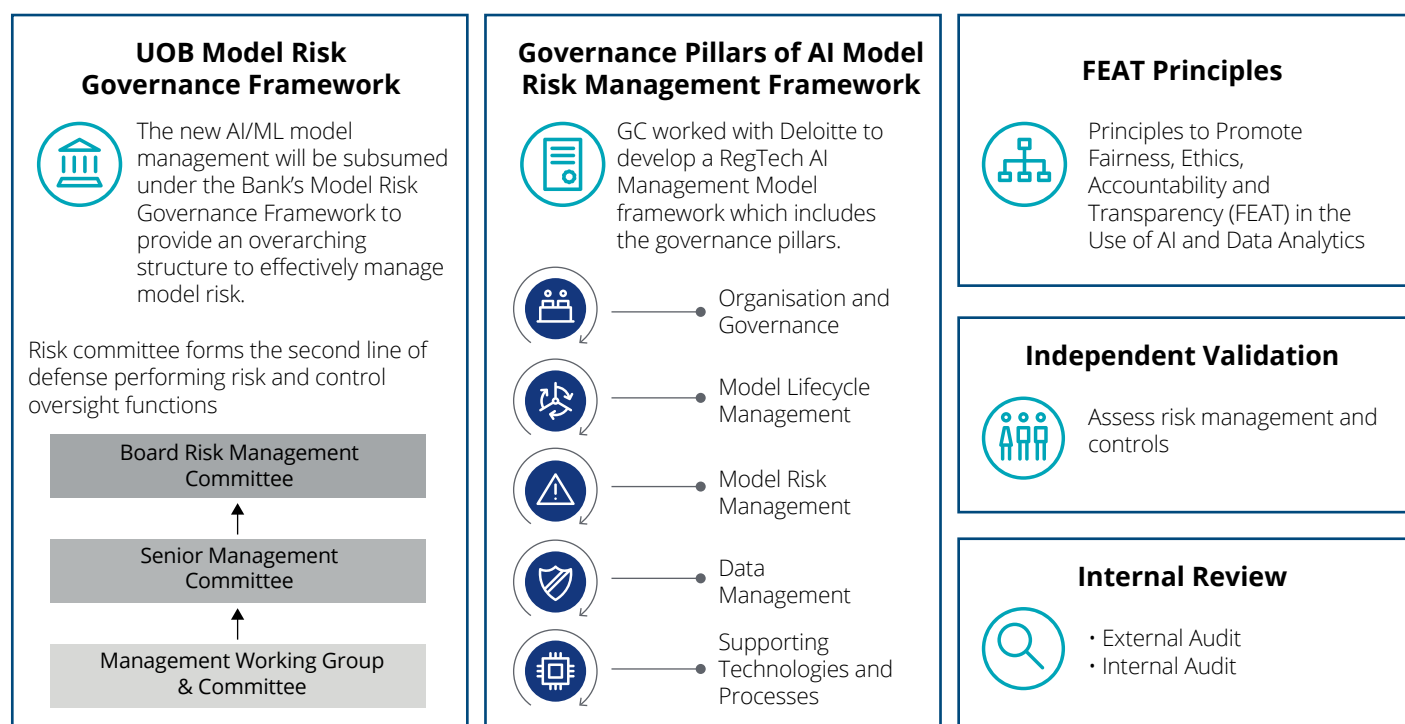
- | | |
|--------------------------------|------------------------------------|
| a) Model risk management | e) FEAT principles |
| b) Managing biases | f) Data management |
| c) Explainability of models | g) Assurance and testing of models |
| d) Application of data privacy | h) Incident resolution |

The objective was for the Bank to mitigate and to manage potential risks from the use of models that might affect its regulatory compliance obligation, customers, shareholder value and reputation.

In preparation for business-live, UOB integrated governing principles into the Bank's business operations and continues to lay out building blocks for effective and sustainable AI/ML governance post business-live. This construct also forms the basis of our validation regime of any model's governance structure.

The key pillars are laid out in Figure 4.

Figure 4: Governance RegTech AI models in UOB



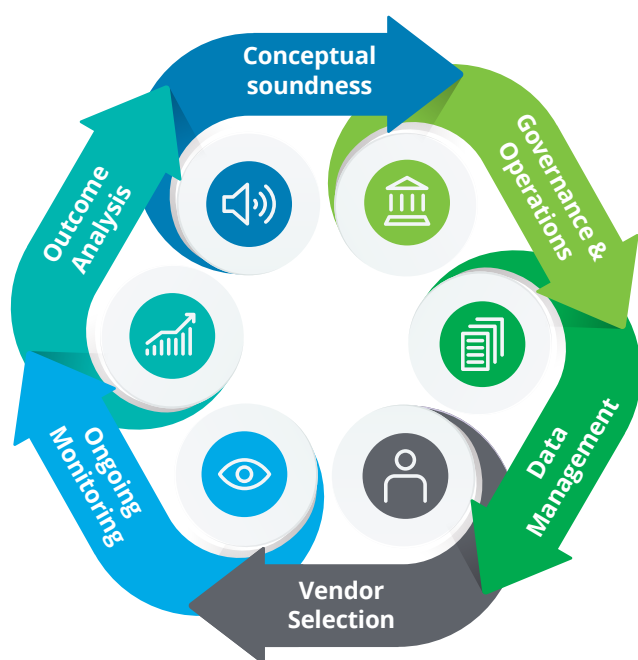
Compliance is about doing things right. A strong risk management and compliance culture demands financial institutions examine how their systems measure up against current threats and the new ways in which criminals seek to infiltrate the financial system. Investing in technologies such as artificial intelligence and analytics are important as they give financial institutions the firepower they need to fight back and to keep the system secure. When UOB began our transformation journey, we did so not to create new technologies, but to ensure we were strengthening our defences. We looked ahead to see what needed to be done to serve customers well, to keep their trust in us as a responsible bank and to exceed their expectations. We have and will continue to be guided by these objectives.

Victor Ngo
Head of Group Compliance, UOB

RegTech AI model architecture validation approach

In addition to robust governance, the model needs to enable the Bank to fulfil desired business objectives and expectations. As such, the second aspect of Deloitte's model management framework provides a comprehensive set of guidelines and dimensions that can be used to approach any model validation exercise. The scope of each validation exercise is dependent on the extent to which models can be tested, the availability of techniques, as well as specific model risk levels. Our validation approach aims to assess the key dimensions set out in Figure 5.

Figure 5: Model architecture validation framework





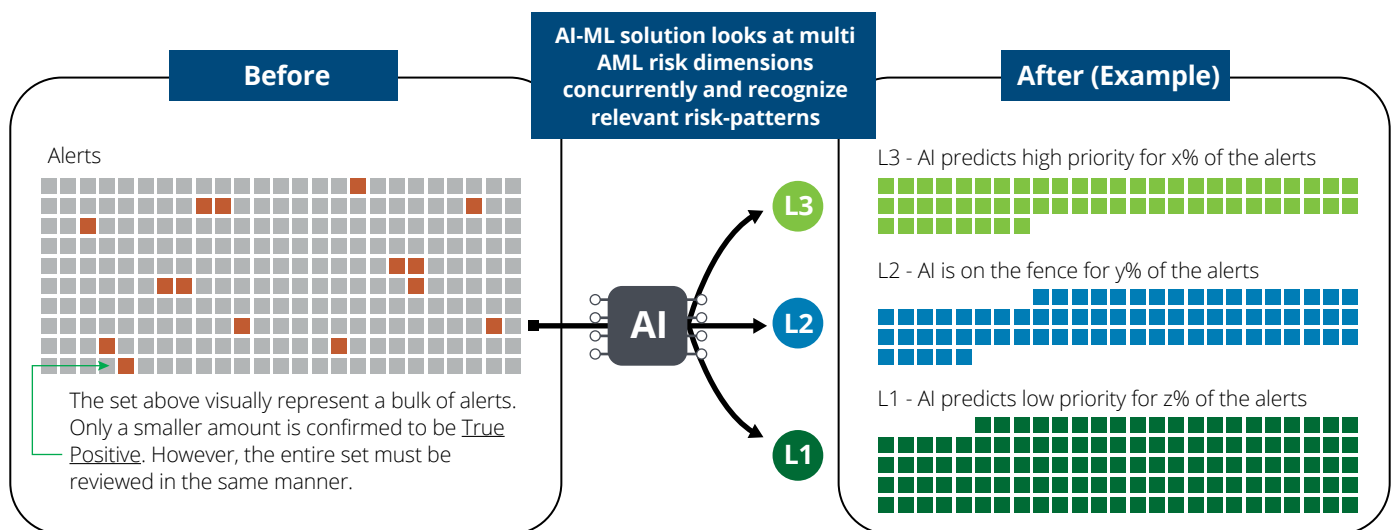
Independent model validations by Deloitte

In preparation for the next step of its business-live process, UOB engaged Deloitte to conduct an independent validation of the technical-live model. This served to evaluate the soundness of the model governance (using the Governance AI Model Management Framework) and solution architecture (via the Model Architecture Validation Framework).

Deloitte's validation revealed positive results for the production model's performance, leading UOB to conclude that it is conceptually sound and robust.

Figure 6 illustrates how the model works conceptually on alerts generated by Transaction Monitoring (TM) and Name Screening (NS) systems.

Figure 6: How the AI/ML model sorts alerts from TM and NS systems

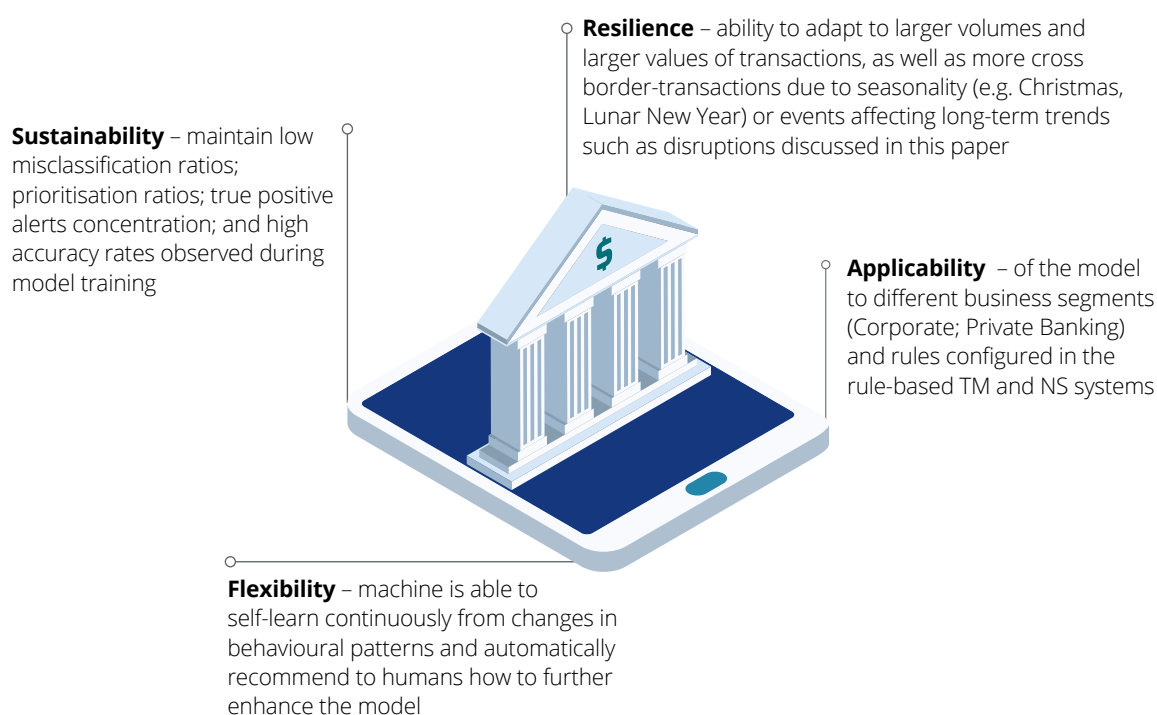


End user validations in UOB

In order to operationalise the model, UOB sought to determine if the model was susceptible to any systematic misclassification of alerts. The Bank conducted an internal review by comparing system-generated results against those performed by the Bank's analysts. Any mismatches were evaluated by the validation team to ascertain if the inconsistencies observed stemmed from machine or human error. The assessment did not reveal major gaps between the model's predictions and output by business users. The conclusion that this had been a successful exercise gave UOB the assurance to implement the model.

Periodic performance monitoring

UOB has instituted a periodic performance monitoring process. This assessment process requires the Bank to examine four key aspects of the model:



We have observed that the model's performance is operating in an optimal range. This is despite an increase in transaction volume when banking transaction patterns shift, or during seasonal fluctuations such as festive seasons.

Model's prediction outcome

During the validation process, we observed that the prediction outcome from the model remained consistent when comparing the results generated during POC and from the parallel run in the actual operating environment.

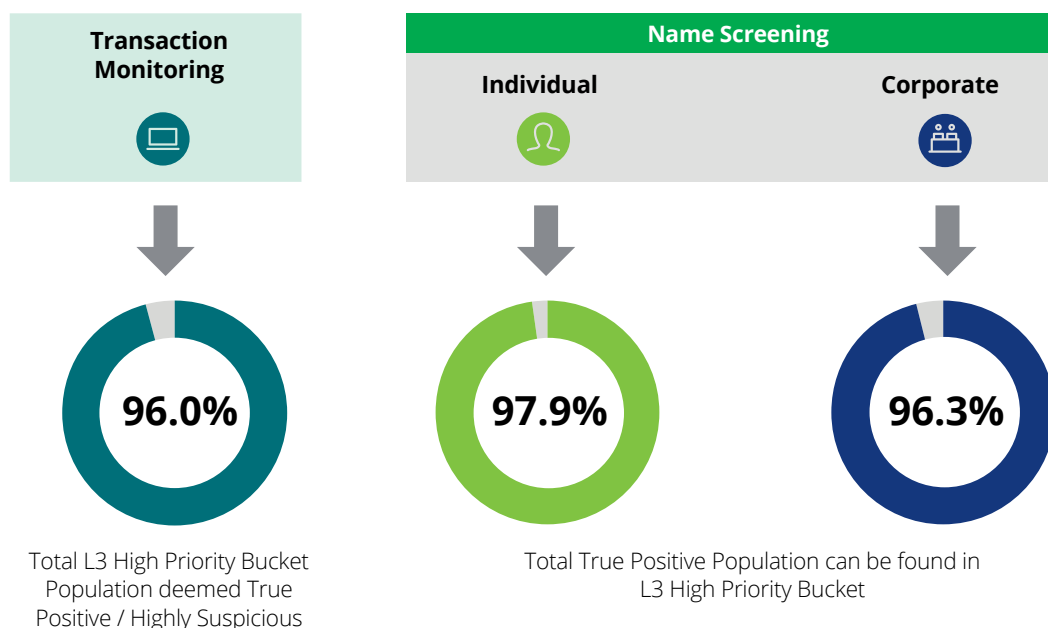
Name screening models

UOB has observed that the NS models for Individual and Corporate customers performed within the prediction boundaries established during POC and Technical-Live stages (set out in our second whitepaper) achieved above **96 per cent** true positive alerts concentration in the High prediction bucket (L3).

Transaction monitoring

The TM model presented positive outcomes with **96 per cent** true positive prediction accuracy in the High prediction bucket (L3) which flags alerts deemed as true positive alerts or highly suspicious. This was achieved due to UOB's TM model relying on thousands of clues (features) when analysing transaction behaviours and predicting the likelihood of true positive alerts. Given these parameters, the model encounters a significantly higher number of instances where the line between a true or false positive is less evident as compared with the NS models.

Figure 8: Results showing the effectiveness of AI/ML models



Engaging stakeholders

Engagement of both internal and external stakeholders has been key to our journey of implementing new technologies to combat financial crime. To help stakeholders trust that these innovations can work reliably and responsibly, we had to ensure they were clear on the operating model of these solutions as well as the outcomes produced.

UOB's initiative is built on the back of the Monetary Authority of Singapore's strong encouragement for financial institutions to leverage technology to combat money laundering and terrorist financing risks. For instance, the use of data analytics can help improve the detection and disrupt criminal behaviour, leading to better support of legitimate businesses. As more financial institutions implement enhanced detection capabilities, coupled with close public-private collaboration in targeting key risks, the financial system will continue to enhance its resilience to financial crime.



Benefits in a time of disruption

UOB: Benefits in a time of disruption

As at the time of publication, the COVID-19 pandemic continues to disrupt economies, industries and businesses across the globe.

UOB, like many other companies, transitioned quickly to remote working without compromising the speed, safety and security of its policies, programmes and processes. This was due to the Bank's ongoing technology investments.

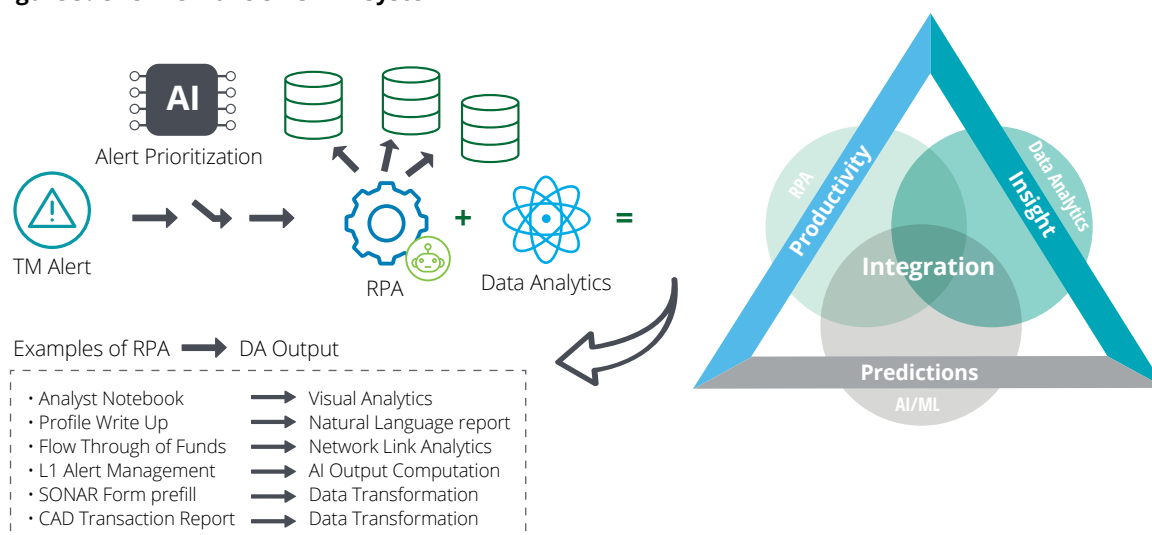
In the area of FCC, UOB's earlier investments and integration of automation and AI into its operating environment meant that the Bank avoided much of the disruption arising from COVID-19. Its technology investments to enhance its systems also enabled the Bank to combat financial crimes effectively, even as illicit activities surged during the pandemic.

- 1) **COVID-19 pandemic:** With greater impetus for a cashless economy amid the pandemic and as cashless transactions continue to grow, existing models used in surveillance systems for FCC need to be recalibrated to reflect the current situation. Typically, such changes can be a lengthy and costly exercise. But this is greatly mitigated now with UOB's ML capabilities. The technology quickly makes sense of data to identify new patterns and insights.

The Bank's use of Robotics Process Automation (RPA) has alleviated manpower constraints for FCC in Singapore, where UOB is headquartered. Robots perform repetitive and computationally challenging work which frees up time for human analysts to make decisions and judgements based on accurate information. Compliance analysts no longer need to generate time-consuming reports manually and on site. This proved useful, particularly during the circuit breaker in Singapore when the Bank's Compliance team was largely working from home. UOB is in the process of implementing RPA in its transaction monitoring process across its global network.

For every alert, the robot extracts customer profile information and transaction data from various systems to form a single report. This is then beefed up using Advanced Analytics and Natural Language Processing to provide greater data points and a visual representation of the customer's flow of funds. It enables analysts to focus their attention on suspicious alerts amid a high alert volume.

Figure 9: Overview of UOB's RPA system





- 2) **ASEAN network connectivity:** Onboarding new customers requires performance of due diligence to identify customers with higher AML/CFT risk profiles. Coupled with strong regional network connectivity, our solution provided a mechanism to enable a more effective identification of extended linkages of customer that may not be apparent at the point of onboarding.

The use of technology in the form of network link analytics (NLA) has proven invaluable in providing a big picture view in the area of TM. NLA examines direct and indirect relationships between customers and their transaction counterparties for the following insights:

- Customer identification – identifying customers with shell company characteristics
- Counterparties' analysis – Understanding customers' counterparties and their transactions with UOB customers.
- Flow of funds – visualising customers' flow of funds and identifying new high-risk transaction patterns and behaviours more effectively

At UOB, we recognised early on the value of insights from complex data sets in enabling us to drive innovation for our customers. In anticipation of the ever-increasing volume and velocity of data that are being generated each day, and integral to our standardised regional technology platform, we designed and built a robust and secure data architecture. On that foundation, we created a data lake at an enterprise level.

In combating financial crime, this unique data architecture enables us to have a holistic view of quality data across all lines of businesses. This means that we are able to test more rigorously and accurately AI/ML solutions within our AML risk management systems to enable swifter and more effective detection of criminals even as they become more sophisticated in their techniques. This is crucial as we continue to invest in technology to enable a safe and secure banking experience for our customers for the long term.

Susan Hwee
Head, Group Technology and Operations, UOB

UOB FCC: The way forward

To drive further innovation in the FCC space, UOB has mapped out five areas of focus for its AML/CFT operations. Its aim is to leverage technology to drive data-driven decision making by compliance officers.

- **Robust Enterprise Applications:** AML/CFT monitoring capabilities have been built into enterprise applications. Instead of just using traditional AML/CFT applications, the Bank can now harness data analytics and machine learning to deepen its understanding of the risk profile and transaction behaviour of customers.
- **Big Data:** AML/CFT data points reside in dozens of enterprise systems across the Bank. A central big data platform aggregates these data for the use of AI/ML in tandem with AML/CFT analytics. Working with technology partners that provide Big Data as-a-service (see figure 10) builds on the Bank's data infrastructure to provide it with the flexibility and scalability to deploy an AI-optimised infrastructure platform in a shorter timeframe. In this regard, UOB partnered Hewlett Packard Enterprise (HPE) to enable the rapid design and deployment of AI solutions such as its Anti-Money Laundering Suite which UOB and Tookitaki co-created. HPE also delivered a public cloud experience which gave rise to better cost effectiveness, control and agility for the Bank.
- **Data Analytics:** With financial systems becoming increasingly globalised, extracting knowledge and insights from AML/CFT data continues to be crucial and can no longer be the skillsets of just a few professionals. The Bank has launched several training programmes, including its flagship learning and development programme for all employees, to train its people to be data conversant. Data champions across all functions and business units are able to tap data dashboards and network analytics tools to analyse and to visualise data to power their decision-making process. Within the Bank's compliance function, efforts are also underway to integrate AML/CFT advanced analytics into other compliance processes.
- **Artificial Intelligence / ML:** AI/ML have been successfully implemented for TM and NS. The Bank is looking to extend the implementation of AI/ML into additional areas such as Sanction Payment Screening and Know Your Customer (KYC) risk profiling.
- **Automation and processes uplift:** Automation, data analytics and AI can make efficient daily compliance operations. RPA can bridge the gap for users looking to use data analytics and AI in everyday decision making.

Figure 10: Big Data as-a-service

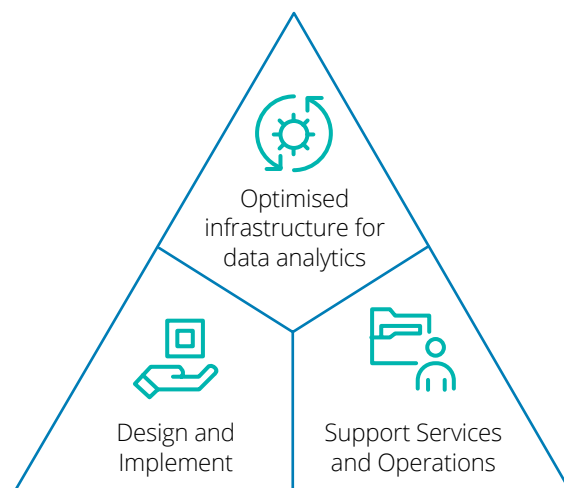
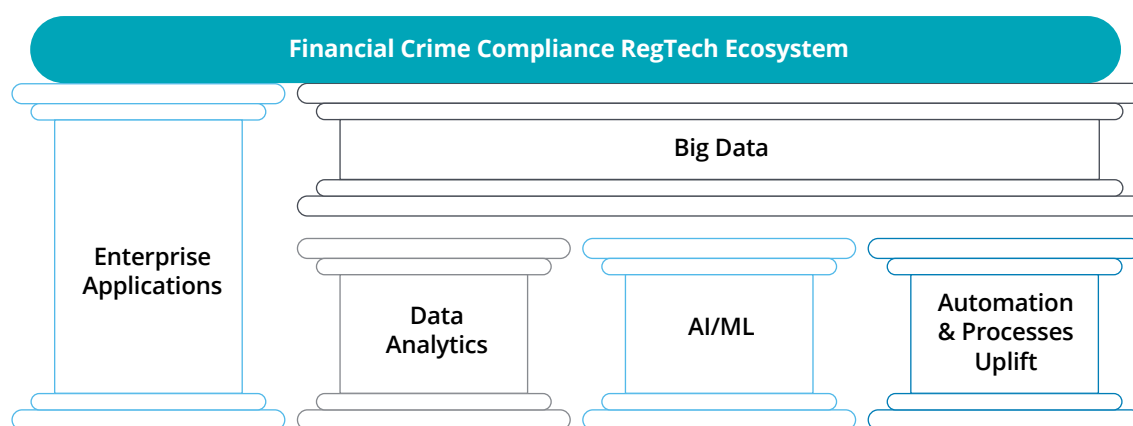


Figure 11: Five Pillars of continuous innovation



The five pillars of continuous innovation in the FCC space cannot exist in silos. UOB has demonstrated through the examples above that they work best in harmony.

The next lap – Integrating AI/ML into financial crime compliance



UOB's point of view

The benefits of advanced analytics and technological innovation play an increasingly crucial role when it comes to fighting financial crime. This extends beyond improving efficiencies and insulating organisations against unexpected macroeconomic events. There is no time more pressing and relevant than now for such technologies to become part of daily operations. UOB's journey has demonstrated that this is both feasible and practical.

The interconnectedness of the financial system makes it even more pertinent for FIs to embrace digital transformation. One weak link in the financial system can result in a global web of suspicious transactions and payments. A multiplier effect in flagging suspicious activities and combating financial crime can be achieved once more FIs adopt new FCC technologies. Stakeholders such as FIs, regulators and independent validators solution architects need to work together as an ecosystem to expand the use of advanced analytics, AI/ML and RPA in areas such as:

- i) monitoring AML customer risk by aggregating customer data from various sources with the help of a centralised data repository;
- ii) monitoring trade-based money laundering (TBML) risks and red flags; and
- iii) effective sanctions payment screening

FCC standards, such as the governance, risk management and maturity assessment standards for use of AI/ML, also need to be strengthened continually with the use of technology to address new threats. Such initiatives should involve a close partnership between the public and the private sectors.

Managing risk is integral to how UOB ensures the sustainability of our business and creates long-term value for our customers and stakeholders. Enabling this is our strong risk management framework, policies and processes as well as investment in technology and innovation. With increased digitalisation comes new dimensions of risks in the area of financial crime and as such technology becomes even more pertinent for FIs to safeguard customers and the financial system. The risk management guidelines which we co-developed with Deloitte provide FIs with a starting point to ensure that robust policies and processes are in place as they tap AI/ML to manage new threats.

Chan Kok Seong
Group Chief Risk Officer, UOB

Holistic surveillance

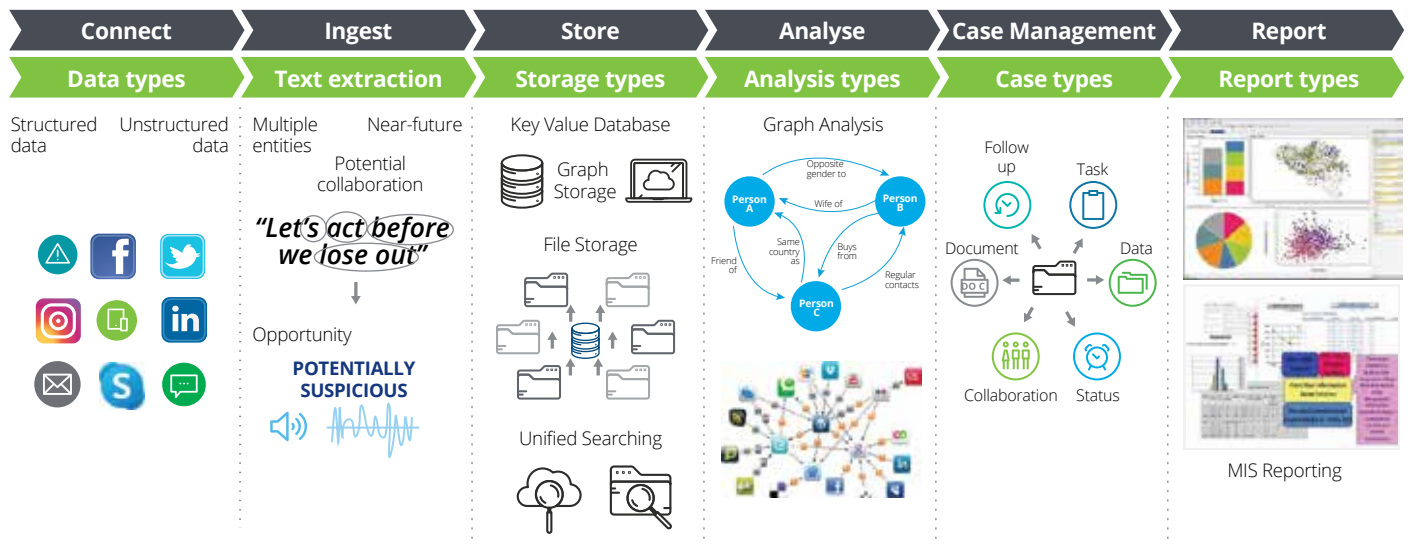
For FIs to make more informed strategic decisions, there is a need to shift the compliance regime from a silos approach to one that is more comprehensive and robust in managing material risks. Such an approach uses “data from all relevant sources within the financial institution to transform the visualisation of financial crime risks.”²

Our envisioned solution architecture

Deloitte’s envisioned holistic surveillance architecture – from the first step of synthesising various data streams to the last step of generating a risk exposure report for end-users – is set out in Figure 12.

FIs need to become more agile in detecting and preventing financial crime and visualising their risk exposure with a customisable dashboard may help this process. The visualisation will provide insights on the connections between data on communication, transactions and behaviour. Both internal (conduct) and external threats can also be examined and flagged for financial crime, in addition to existing monitoring and screening efforts.

Figure 12: Holistic surveillance architecture



Conclusion



The continued effective detection and prevention of financial crime requires ongoing effort and investment in operationalising technologies such as automation, advanced analytics and AI in the mainstream FCC framework. The COVID-19 pandemic has also underscored the need to adopt these tools to improve adaptability and agility demanded by an increasingly connected world defined by constant change, disruption and global events. FIs that have incorporated technologies for FCC would find they are more adept during these trying times to mitigate risks. This has been the case for UOB.

Ensuring a robust FCC programme is an ongoing effort given that criminal behaviours continues to morph and become more complex as bad actors take advantage of the changing, more disrupted and more connected world. This in turn demands compliance functions to be as agile to put in preventative measures to ensure that financial system does not become a conduit for illicit activities. Recent events have demonstrated that employing the use of AI/ML and RPA has enabled UOB to ride through such challenges with greater ease and emerge on better footing.

Beyond meeting BAU needs, investment in these innovations has carried greater benefits in unprecedented circumstances such as the COVID-19 pandemic, as seen from UOB's journey thus far. Set within the context of heightened regulatory focus and FCC requirements coupled with limited resources in FCC functions, FIs have been tasked to do more with less in the fight against financial crime. With that in mind, the application of innovation such as the use of AI/ML models for NS and TM represents the dawn of more effective compliance regimes and ushers the rise of wider and deeper application of technologies as mooted above. Moving into a post-pandemic world, the industry may wish to take the same steps as organisations such as UOB and other technology-oriented FIs to stay relevant and ready to combat new waves of financial crimes regardless of peace-time or disruption.

We summarise key areas as being the following:

- 1) Encouraging an FCC maturity model – creating an industry-wide agreed standard for benchmarking of an FI's progress and reaching a consensus on the general direction of development will provide an implementation roadmap for reference.
- 2) Ensuring a robust model governance – governance frameworks with high levels of granularity tailored for unique models as well as individual FIs' wider governance structures should be developed, based on FCC regulatory expectations, controls and robust risk management standards.

The potential of these innovations can only be fully realised when robust and adequate governance, as well as risk management, are embedded within the innovation framework. This is a fundamental and vital step towards widespread operationalisation and its importance cannot be emphasised enough.

Tapping innovative technologies enable FIs to take a step forward, towards the vision of holistic surveillance. Once the FI has established robust governance frameworks across all models, technology solutions can create a layer over existing systems in the FI to bring together a wide range of data and to provide senior management with a 360-degree view of risks across the organisation. This will not only provide greater transparency on the inherent and residual risks in the business, but also ensure that FIs tap into all available data while making risk decisions.

In our view, the use of AI/ML and RPA enhances the risk management capability of an FCC programme. This will bring about the resultant effect of greater trust in the FI by its customers, regulators and other stakeholders.

While new disruptions undoubtedly pose serious threats to FIs, they also present FIs with the opportunity to accelerate the development of new FCC capabilities and tools.

As evidenced by those that have worked to stay ahead of the curve, what is needed are industry-wide efforts and close collaboration of stakeholders to concretise the pathway to thriving FCC functions in this new world.

As explored in our series of whitepapers, the future of FCC is not a distant yonder – it is here now for adoption, creating a systematically interwoven community that combats financial crime with sharpened capability and deep trust in the system.

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) Radish Singh, Min Liu, Nick Lim, Eric Ang, 'The Future of Financial Crime Compliance A Compelling Use of Innovation in a Converging Digital and Physical World', Volume 2, November 2019, Deloitte and UOB, <https://www2.deloitte.com/sg/en/pages/financial-advisory/articles/financial-crime-compliance.html>
- 3) Yuan Yang, Edward White, Robin Harding, Kiran Stacey, Clive Cookson, Najmeh Bozorgmehr, Miles Johnson, Steve Bernard, Jack Francklin, 'How countries around the world are battling coronavirus', Financial Times, March 10, 2020, <https://www.ft.com/content/151fa92c-5ed3-11ea-8033-fa40a0d65a98>
- 4) FATF, 'COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses', May 2020, <https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf>
- 5) IDC, 'IDC Forecasts Strong 12.3% Growth for AI Market in 2020 Amidst Challenging Circumstances', August 4, 2020, <https://www.idc.com/getdoc.jsp?containerId=prUS46757920>
- 6) Fintechnews Singapore, '3 in 4 Banks in Asia Will Invest in Machine Learning This Year', April 23, 2019, <https://fintechnews.sg/30005/ai/refinitiv-ai-and-machine-learning-to-transform-financial-services/>
- 7) SAS, 'Where human capabilities fail', https://www.sas.com/en_us/customers/allianz-fraud-management.html
- 8) Priyankar Bhunia, 'Enhancing customer journeys and improving fraud detection through machine learning', April 13, 2018, <https://www.opengovasia.com/enhancing-customer-journeys-and-improving-fraud-detection-through-machine-learning/>
- 9) Soumik Roy, 'How artificial intelligence is fighting financial crime', June 17, 2019, <https://www.fintechnews.org/how-artificial-intelligence-is-fighting-financial-crime/>
- 10) S Iswaran, 'Singapore Statement by Mr S Iswaran, Minister for Communications and Information, at the G20 Digital Economy Ministers Meeting', July 22, 2020, <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/7/singapore-statement-by-minister-iswaran-at-the-g20-digital-economy-ministers-meeting>

- 11) European Commission, 'On Artificial Intelligence - A European approach to excellence and trust' February 2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
- 12) Russell T. Vought, 'Guidance for Regulation of Artificial Intelligence Applications', The White House, <https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>
- 13) Tim Adams, Andres Portilla, Matthew Ekberg, Michael Shepard, Rob Wainwright, Katie Jackson, Tamsin Bauman, Chris Bostock, Abu Saleh, Pablo Sapiains Lagos, 'The global framework for fighting financial crime Enhancing effectiveness & improving outcomes' October 2019, IIF and Deloitte, <https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html>
- 14) Monetary Authority of Singapore, 'MAS introduces new FEAT Principles to promote responsible use of AI and data analytics', November 12, 2018, <https://www.mas.gov.sg/news/media-releases/2018/mas-introduces-new-feat-principles-to-promote-responsible-use-of-ai-and-data-analytics#:~:text=The%20Monetary%20Authority%20of%20Singapore,and%20data%20analytics%20in%20finance>
- 15) Monetary Authority of Singapore, '"Fairness Metrics" to Aid Responsible AI Adoption in Financial Services', May 28, 2020, <https://www.mas.gov.sg/news/media-releases/2020/fairness-metrics-to-aid-responsible-ai-adoption-in-financial-services>
- 16) Monetary Authority of Singapore, 'MAS Partners Financial Industry to Create Framework for Responsible Use of AI', November 13, 2019, <https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai>
- 17) Eric Charran, Steve Sweetman, 'AI Maturity and Organizations – Understanding AI Maturity' Microsoft, <https://www.bastagroup.nl/wp-content/uploads/2019/01/AI-Maturity-and-Organizations-eBook.pdf>
- 18) Svetlana Sicular, Bern Elliot, Whit Andrews, Pieter den Hamer, 'Artificial Intelligence Maturity Model', March 2020, Gartner, <https://www.gartner.com/guest/purchase/registration?resId=3885363>
- 19) Deloitte, 'IIF and Deloitte White Paper Outlines Needed Reforms to Improve the Global Framework for Fighting Financial Crime, October 16, 2019, <https://www2.deloitte.com/global/en/pages/about-deloitte/press-releases/iif-deloitte-paper-on-fighting-financial-crime-pr.html>

Contact us

Radish Singh

Financial Crime Compliance Leader and AML Partner
Financial Advisory
Deloitte Southeast Asia

✉ radishsingh@deloitte.com

Nicholas Alvin Sebastian

Director
Financial Advisory
Deloitte Southeast Asia

✉ nicsebastian@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 refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.