Regtech Adoption Practice Guide

Issue #6: Artificial Intelligence-based Regtech Solutions

April 2022

HONG KONG MONETARY AUTHORITY
香港金融管理局

KPMG

Disclaimer

Regtech Adoption Practice Guide is a publication published by the Hong Kong Monetary Authority (HKMA). It should be noted that the sole purpose of this publication is to provide Authorized Institutions (banks) with information on the latest regulatory technology (Regtech) developments. The HKMA does not endorse any use cases, solutions and/or implementation guidance described in this adoption practice guide. If a bank intends to adopt a particular solution or implementation, it should undertake its own due diligence to ensure that the technology or approach is suitable for its circumstances.

Contents

1 Introduction **4**

1.1 Background 4

1.2 Purpose 5

2 Artificial Intelligence-based Regtech adoption **6**

2.1 Key developments 6

2.2 How can AI-based Regtech solutions help? 7

2.3 Key barriers/risks when adopting AI-based Regtech solutions 8

3 Implementation guidance **10**

3.1 Pre-requisite 1: Establish organisational data governance 10

3.2 Pre-requisite 2: Establish an AI governance framework 12

3.3 AI-based Regtech solution implementation 14

4 Regtech use cases **16**

4.1 Use Case #1 – Automated supervision of financial product sales process against regulatory requirements 16

4.2 Use Case #2 – Federated Learning technology to enable bankruptcy detection 17

A Appendix **20**

A.1 Acknowledgements 20

A.2 Relevant regulatory requirements and/or guidance 20

01 Introduction

1.1 Background

The value of Regtech in banking is coming to the fore in Hong Kong, offering clear benefits to banks, customers and regulators. In November 2020, the HKMA released a two-year roadmap to promote Regtech adoption in Hong Kong, as laid out in a White Paper titled "Transforming Risk Management and Compliance: Harnessing the Power of Regtech".[1] The White Paper identified 16 recommendations across five core areas to accelerate the further adoption of Regtech in Hong Kong.

The White Paper acknowledges that since 2019, the HKMA has published a series of "Regtech Watch" newsletters, introducing banks to Regtech use cases on the adoption of innovative technology to enhance risk management and regulatory compliance. The banks interviewed for the White Paper cited these newsletters as a valuable source of information and guidance, especially the actual or potential Regtech use cases that have been rolled out or are being explored in Hong Kong or globally.

The White Paper identified 26 specific application areas of Regtech that can benefit banks. There are significant opportunities and a strong desire from the industry for the HKMA to develop and issue "Regtech Adoption Practice Guides" around these application areas.

As a successor, this Regtech Adoption Practice Guide (Guide) series builds on the "Regtech Watch" newsletters to include common industry challenges, guidance on implementation and examples of what others have done successfully to overcome adoption barriers. The Guides are to supplement other ongoing HKMA initiatives such as the Banking Made Easy initiative, Fintech Supervisory Sandbox and the Fintech Supervisory Chatroom. Ultimately, the Guides should enhance the sharing of experience related to Regtech implementation in the industry, which will help further drive Regtech adoption in Hong Kong.

Regtech solutions are expected to become increasingly powerful as the underlying technologies mature. This sixth Guide of the series focuses on the adoption of

[1] Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf

"Artificial Intelligence-based (AI-based) Regtech solutions" in banking. As Artificial Intelligence (AI) technologies evolve and mature, they are expected to enable the creation of more powerful solutions. When applied to banking, AI technology can enable the automation of business processes, detect patterns, generate insights and drive engagement with customers and employees through targeted communications.

1.2 Purpose

The purpose of this Guide is to provide an overview of AI-based Regtech solutions, outline the common challenges observed during implementation and share experience on how others have addressed the challenges to successfully adopt Regtech solutions in their organisations. This Guide follows the outline below:

1 **Explain how AI-based Regtech solutions can be used to support risk management and regulatory compliance**

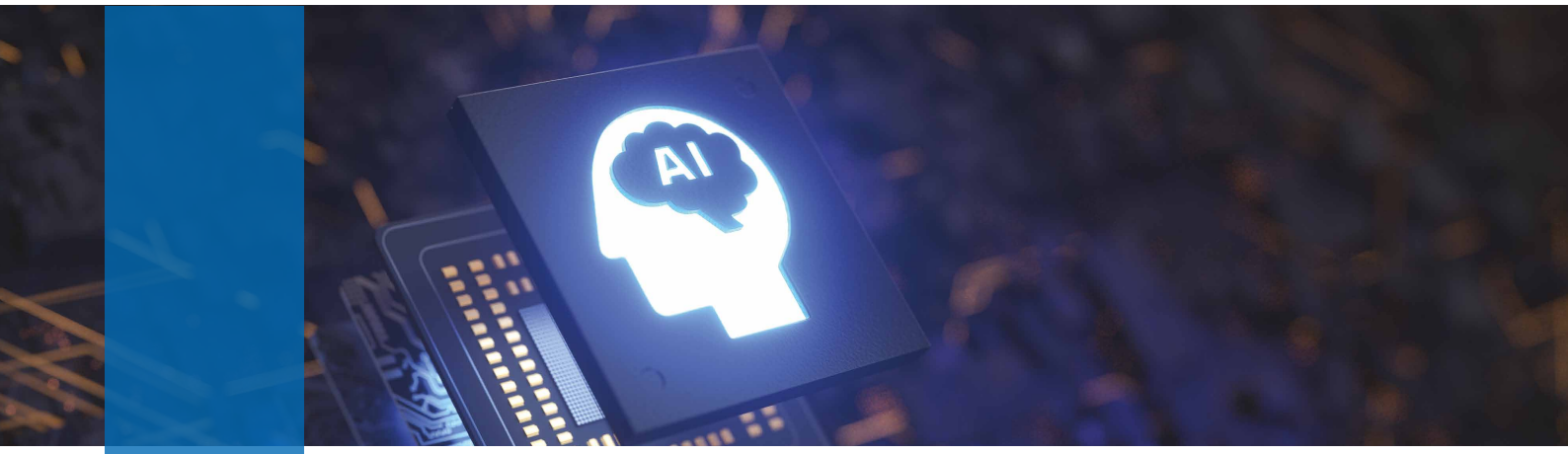
- Illustrate the benefits of leveraging AI-based Regtech solutions
- Describe key barriers/risks when adopting AI-based Regtech solutions

2 **Provide practical implementation guidance to banks on the adoption of AI-based Regtech solutions**

- Outline key components of AI-based Regtech solution implementation, with a particular focus on the key barriers/risks of adopting AI-based Regtech solutions for banks

3 **Share use cases on the adoption of AI-based Regtech solutions**

- Describe the challenges faced by a bank and how the Regtech solution helped to resolve these challenges
- Outline the key learnings from successful AI-based Regtech implementation



02 Artificial Intelligence-based Regtech adoption

2.1 Key developments

AI is an overarching concept that refers to different emerging technologies mimicking the cognitive functions of humans, such as problem-solving, speech recognition, visual perception, decision-making and language translation. Many banks in Hong Kong realise the benefits of utilising AI to improve banking functions. The application of AI can improve the efficiency and effectiveness of internal processes and risk management (e.g. operational automation, fraud prevention, and detection) as well as enhance customer experience (e.g. chatbots, personalised products to suit customer needs, and risk profiles).

The breadth of AI applications in the banking industry is increasing. Advances in AI and automation technologies have allowed for the development of Regtech solutions that address a wider spectrum of risk management and compliance areas (please refer to Table 1 for an overview of AI technologies and examples of Regtech applications).

Table 1: AI technologies supporting Regtech solutions

Technology	Description	An example of Regtech application
Artificial Intelligence (AI)	A set of technologies that mimic the cognitive functions of humans such as decision-making	AI acts as the underlying technology for many Regtech solutions including data analysis, regulatory monitoring and forecasting
Machine Learning (ML)	ML is a subset of AI techniques that can train and improve algorithms based on large datasets without human intervention	ML models that are trained on client financial data can enable the automation of credit decisions
Federated Learning	A form of ML which allows different parties to collaboratively train models using multiple datasets without the need to share proprietary data	A Federated Learning platform that allows multiple banks to collaboratively build a bankruptcy detection model without exposing the data (for more details, please see Use Case 2 in Section 4.2 of this paper)
Natural Language Processing (NLP)	As a branch of AI, NLP transforms unstructured data such as text or voice recordings into structured data so that human languages can be understood by a computer	A NLP-based sales compliance solution that can convert customer calls to structured text for supervision against regulatory requirements (for more details, please see Use Case 1 in Section 4.1 of this paper)
Intelligent Process Automation (IPA)	Combines the capabilities of Robotic Process Automation (RPA)[2] and AI to automate repetitive tasks, analyse complex processes and make process suggestions	An IPA tool that can analyse a large volume of regulatory documents which triggers a workflow to assess the impact and summarise next step actions

2.2 How can AI-based Regtech solutions help?

AI can be applied to the risk management and compliance operations of banks to streamline processes, alleviate manual workloads, enable the detection of patterns, actively monitor risks, and predict compliance issues. This section, while not exhaustive, outlines the possible areas where AI-based Regtech solutions can be leveraged to address common challenges faced by banks:

Manual processes: Traditionally, banks' regulatory activities are highly manual, prone to human errors, slow and inefficient processes, and unexpected spikes in resource requirements can lead to a strained workforce. Banks are increasingly using Regtech solutions, particularly those powered by AI, to achieve scalability in their operations and reduce manual effort.

IPA combines the capabilities of RPA with AI technology to replicate the human cognitive function to analyse complex processes or interpret text-heavy workloads to make process suggestions to users. A use case for IPA in banks is the detection of changes in regulations by analysing regulatory documents and subsequently triggering a workflow to assess the impact and summarise the required change.

Greater regulatory expectation on the scope of control activities: Regulators increasingly expect control activities within banks to be highly effective at identifying instances of regulatory breaches – traditional testing approach of a small sample of control execution does not satisfy the growing expectation.

AI can help banks to monitor all transactions and process large amounts of internal and external regulatory data in an efficient manner. For example, NLP and voice analytics can be used in the monitoring and surveillance of employees so that potential compliance issues can be identified. This helps the bank to detect and prevent potential compliance breaches in a timely manner.

An increasing volume of transactions: The increase in electronic transactions over cash transactions calls for a greater need for automated and AI-based solutions to effectively detect fraudulent activities. Examples include the use of Regtech solutions to monitor customer transactional activities, enabling the automated detection of suspicious transactional behaviour and patterns[3].

[2] RPA uses software bots to automate a series of repeatable tasks or workflows by using clear processing rules and a definite set of possible outcomes. Whilst RPA does not specifically use AI, it lays the foundation for AI use and its rule-based software bot can be built and configured with AI to provide deeper context in an automated series of processes.

[3] Regtech Adoption Practice Guide Issue #2: Anti-Money Laundering / Counter-Financing of Terrorism, HKMA (July 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210726e1a1.pdf

Increasing amount of data sources with broader usage: As banks are collecting and storing increasing amounts of data, an ML model can help to predict possible outcomes through iterative processing and analysis of a large datasets. For example, an investment risk model may find externally available company attributes such as expenses, income, historical regulatory related fines, and internally held data such as loan pay-back ability to correlate and calculate the investment risk. The data in turn helps to train a model that can enable automated investment decisions.

As AI solutions require a significant volume of quality data, many banks face challenges in the availability and quality of their data due to factors such as unidentifiable and duplicated data sources, duplicated data storage locations, lack of data ownership, poor data quality, unstructured data, and manual data verification and reconciliation. AI can help streamline and better control the gathering of source data from different systems across a bank as detailed in Regtech Adoption Practice Guide Issue #4: Regulatory Reporting and Stress Testing[4].

Increased customer expectations: COVID-19 has accelerated the adoption of digital technologies. Customers have become accustomed to receiving products and services digitally and are increasingly expecting the same frictionless digital experience from their banks.

AI solutions can streamline the customer journey to provide an enhanced experience, whilst continuing to manage a bank's risk and meet compliance obligations. For example, NLP and ML-based sales compliance solutions can be used to minimise multiple call-backs to customers (for more details please see Use Case 1 in Section 4.1 of this paper).

Other challenges that can be addressed by AI-based Regtech solutions include dealing with increasing regulatory complexity, managing the associated costs of compliance, and meeting greater expectation on control and system auditability.

2.3 Key barriers/risks when adopting AI-based Regtech solutions

Whether AI-based Regtech solutions are developed in-house or by vendor partners, it is important for banks to establish proper governance and controls to manage the related risks. Some of the key barriers and risks for AI-based Regtech solution adoption are listed below. **Section 3** of this Guide **("Implementation Guidance")** will further explore the methods banks may adopt to overcome these barriers and mitigate or minimise the impact of the key risks.

Key barriers

- **Data availability and quality:** The effectiveness of AI applications depends on the availability of high-quality, diverse, and dynamic datasets. Banks should therefore have the right data infrastructure in place (e.g. a data lake hosting data from multiple source systems) to ensure that all the relevant internal and external data are available and current. However, the maturity of data infrastructure varies amongst banks, with time and monetary investment required to build up the necessary infrastructure.

  Poor data quality has a direct correlation to inaccurate and biased results. Due to the complexity of the data lineage and frequent changes in data ownership, banks often find it challenging to locate the data sources, conduct data validation, and maintain data quality.

[4] Regtech Adoption Practice Guide Issue #4: Regulatory Reporting and Stress Testing, HKMA (November 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20211126e1a1.pdf

- **Talent and relevant skillset shortage:** Talent and relevant skillset shortage has been identified as a significant barrier to Regtech adoption across the HKMA White Paper, the Regtech Adoption Index[5], and the Regtech Skills Framework[6] report. AI is a fast-moving topic, and developments in AI-related skillsets are constantly progressing. Emerging domains that require innovation – such as AI-enabled Regtech – are still experiencing a large skills gap. If banks are unable to secure talent with cross-disciplinary skills or upskill existing employees, they will find it difficult to adopt AI-based Regtech solutions.

- **Adoption of Cloud computing:** Cloud computing provides the data storage capacity and massive processing power that are fundamental to AI innovation. Many AI-based Regtech solutions available in the market are also cloud-based. Although Hong Kong-based banks have started to adopt Cloud computing, this is still at a relatively early stage, as detailed in the first Regtech Adoption Practice Guide "Cloud-based Regtech solutions"[7].

Key risks

- **Data Privacy and right of use:** AI-based Regtech solutions are reliant on the ingestion of vast amounts of data to train models and detect patterns. Depending on the Regtech application areas, the data utilised by AI-based Regtech solutions may involve personal data. Related data privacy risks include:

  – Excessive data are collected than required

  – Data are used for purposes other than specified

  – Data are stored and transmitted insecurely

  – Risks of discrimination and profiling[8]

  When adopting AI-based Regtech solutions that involve personal data, banks need to conduct a comprehensive privacy risk assessment, referencing the Data Protection Principles under the Personal Data (Privacy) Ordinance. Banks should also ensure good data ethics within the development and operation of AI-based Regtech solutions.

- **Accuracy and reliability:** While some AI models can make judgements/decisions with minimal human interference, banks need to be aware that outputs can be biased and can lose accuracy over time. Outcome bias is often the result of a stale dataset or when certain populations are under/over-represented in the data. In addition, AI model performance will degrade over time due to various reasons, such as when previously unseen data become available, or variables and parameters change triggered by a change in the business and upstream data changes.

  Banks should be mindful of such limitations and plan and execute continuous monitoring after deploying AI models to detect performance degradation, known as model drift, and ensure the models are continuously trained and updated to remain accurate and applicable.

- **Explainability:** While AI-based solutions offer significant automation opportunities, there is a major risk for the growing AI sophistication, i.e. explainability. The lack of understanding of how AI-based solutions work to produce output is also referred to as a "black box" risk.

  AI-based Regtech solutions outputs are often tied to risk management decisions or compliance outcomes. Banks should implement adequate measures to ensure an appropriate level of transparency and explainability commensurate with the materiality of the solutions.

[5] The Regtech Adoption Index 2020, HKMA (June 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2021/20210617e5a1.pdf
[6] Regtech Skills Framework - Assessment & Recommendations Report, HKMA (October 2021)
[7] Regtech Adoption Practice Guide Issue #1: Cloud-based Regtech Solutions, HKMA (June 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2021/20210617e5a1.pdf
[8] Guidance on the Ethical Development and Use of Artificial Intelligence, Office of Privacy Commissioner of Personal Data, (August 2021), https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf

03 Implementation guidance

Before implementing an AI-based Regtech solution, banks should establish a proper enterprise-level data AI governance model as well as ensure access to AI-related skills and capabilities. Banks can establish talent programmes to upskill staff based on recommendations outlined in the Enhanced Competency Framework on Fintech[9] and Regtech Skills Framework published by the HKMA. This section outlines some pre-requisites and key considerations for AI-based Regtech implementation to address the challenges and barriers listed in Section 2.3.

3.1 Pre-requisite 1: Establish organisational data governance

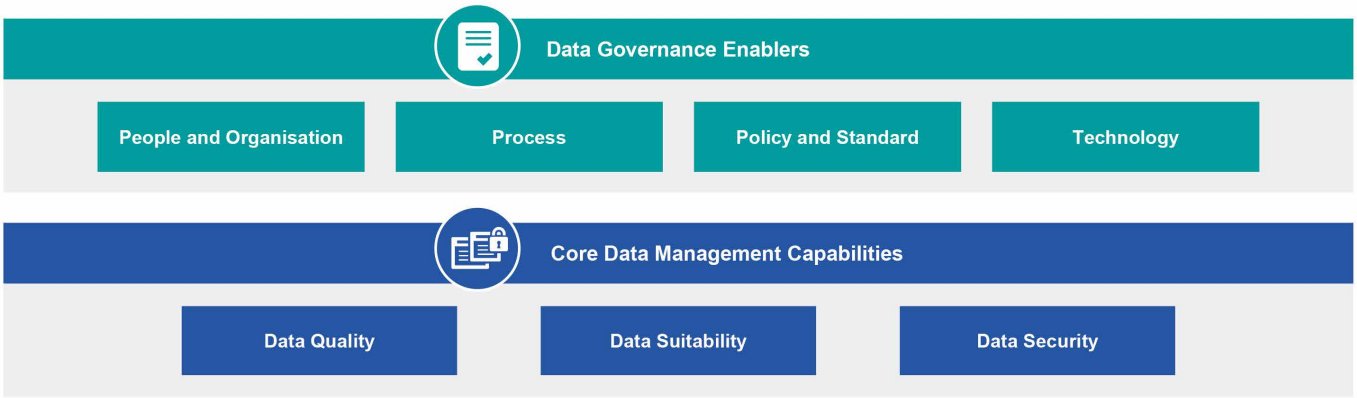
Data governance is an enterprise-wide standardisation of roles, processes, policies, and standards in regard to data. A lack of standardised data governance results in a cumbersome and time-consuming process to identify and extract the relevant data when required. Proper data governance provides an effective foundation and best practices for banks to deploy AI-based Regtech solutions. Without this foundation, AI-based Regtech solutions would be built upon unsuitable poor quality data, which could lead to inaccurate outputs, greatly reducing the value such solutions could bring to a bank.

Data governance components

As a first step, a bank should define its data governance components. Below are some critical components that banks should consider including in their data governance programme:

[9] Enhanced Competency Framework on Fintech, HKMA (December 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20211203e1.pdf

Figure 1: Data governance components for AI-based Regtech solutions



- **People and organisation:** Buy-in from the senior leadership is key to a successful data governance programme. Once the executive sponsorship is obtained, a data governance committee should then be formed to drive data management activities. As each business unit uses data differently, it is critical that the committee comprises data owners from diverging lines of business as well as the IT departments. Banks should also invest in training employees in key data capabilities, such as business intelligence, advanced analytics, data architecture, and data integration to prepare the organisations for change.

- **Process:** Establishing and standardising data governance processes is essential for the effective execution of data management activities. Typical data governance processes include request management and issue resolution.

- **Policy and standard:** A data governance policy is a set of standardised guidelines, operational procedures, and management approaches to manage data throughout the entire data lifecycle, from creation to disposal. To ensure consistent execution of data management, quantifiable standards should also be defined.

- **Technology:** Technology facilitates the access to and management of data as well as adherence to processes and procedures. Banks need to modernise their data architecture before realising the benefits of AI technology. Banks should also identify data tools and platforms for the monitoring and consumption of data by business units across the banks.

- **Data quality:** Data quality determines the outcomes of an AI application. Banks should therefore establish a data quality framework comprising processes to review and address data quality issues.

- **Data suitability:** Banks must ensure the data are fit for purpose and that they represent a sizable sample that accurately reflects the overall data population.

- **Data security and privacy:** Data privacy refers to safeguarding banks' enterprise and customer data throughout the data management lifecycle. Banks should define and establish rules and controls on the authentication, authorisation, and access to data at the raw data level. All data activities, for example, access to and modifications of data, should be properly recorded to fulfil audit requirements.

All business units across the bank and IT departments need to be involved to establish the right organisational data governance. A bank can consider the three-step approach outlined below to establish organisational data governance:

1. **Understand the current state:** The first step is to understand the current practices across the above data governance components before defining the strategy and vision of the future state. A review of data inventory should be performed to understand where data resides across the organisation. This can be done through a documentation review and interviews with data owners or subject matter experts from the business functions. The exercise also allows banks to better manage data-related risks such as data breach or leakage of customer data[10]. Interviews should focus on capturing the as-is state as well as understanding the current use cases, pain points, and potential data requirements for the future.

[10] Sound practices for customer data protection, HKMA (April 2022), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220404e1.pdf

2 **Design and build a data governance framework:** The data governance framework should be designed with consideration of the existing business landscape and future-state vision against all relevant data governance components. Key business users should be involved throughout the design process and key stakeholders should be engaged early to socialise the design. This enables users to be aware of the design and generates buy-in.

3 **Implement the data governance framework:** The implementation stage will enable the bank to bridge the gap between the current state and the target data governance framework. The key to implementation is a well-designed and realistic implementation roadmap which should be developed based on prioritised initiatives and take into account any dependent activities. The implementation should be managed as a project using a clearly defined project delivery methodology.

3.2 Pre-requisite 2: Establish an AI governance framework

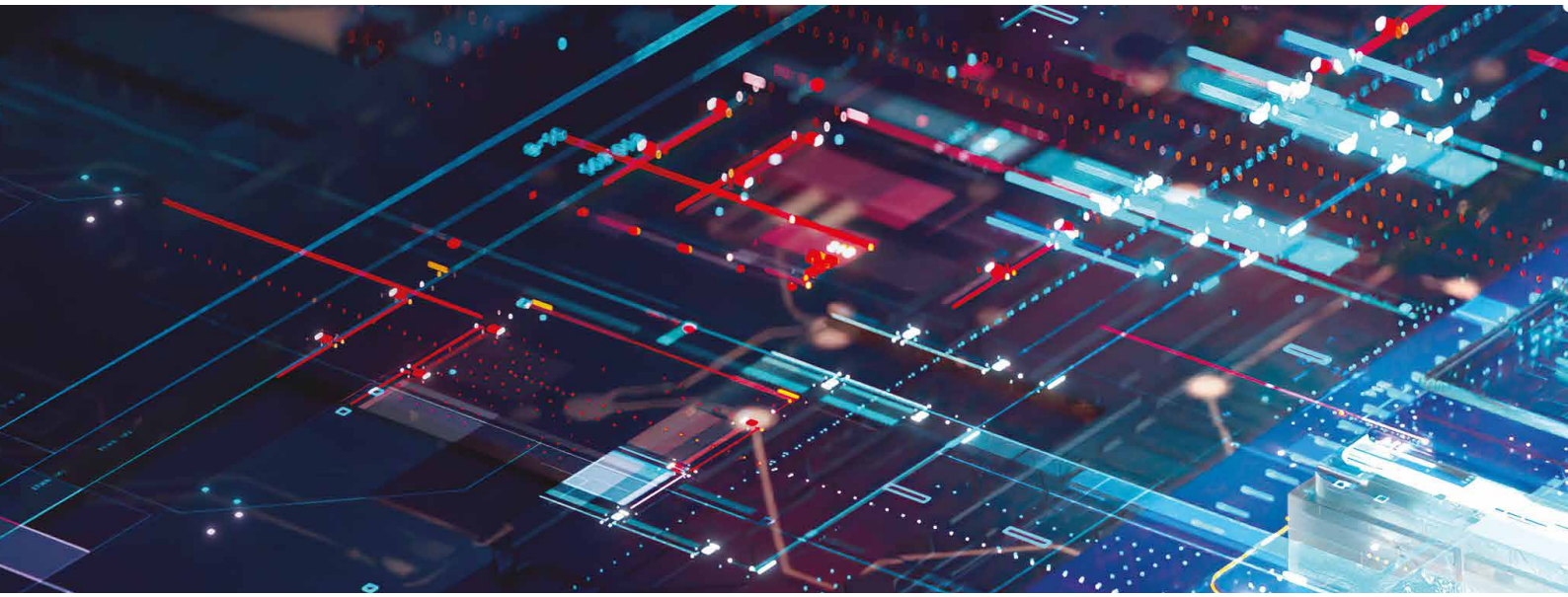
A robust AI governance framework enables and operationalises trust, accountability, and transparency in AI-based solutions. Currently, there is no industry-standard AI governance framework. However, various organisations, including the Office of the Privacy Commissioner for Personal Data in Hong Kong and the HKMA have published guidance on AI governance and high-level principles on AI[11], which banks could reference when establishing their AI governance framework. While not exhaustive and applicable to all AI-based Regtech solutions, this section captures some key steps banks can consider when establishing their own AI governance framework.

Understand the current state: Identify and document all AI-based solutions in the organisation to understand existing AI use cases and capabilities. Gather and assess any current governance and risk frameworks applied to AI-based solutions and identify areas of focus.

Develop a strategy and governance: Banks, whether developing their own AI solutions or working with third-party vendors, should develop AI-related strategies, principles, and controls that generate trust in the solutions. Where possible, banks should obtain documentation from third parties to ensure adherence to their AI principles. Examples of AI principles that promote trust are:

- **Algorithm integrity:** Confidence in the validity of training data and processes and metrics used to develop and evaluate AI solutions.
- **Explainability of the algorithmic decision-making process:** Understanding why and how the AI models produce the outputs promotes transparency and reliability.
- **Fairness of the models:** Consideration of bias, such as race and gender, to ensure the models are inclusive and free from prejudice.

[11] High-level Principles on Artificial Intelligence, HKMA (November 2019), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf



- **Resilience:** Refers to the ability of the AI solutions to withstand a major disruption within acceptable degradation of performance and to recover within an acceptable time frame.

Define a target operating model (TOM): Creating an AI TOM and subsequent implementation of the TOM help banks to understand how the AI solutions will be managed and run. Key components to include in the AI TOM are:

- The identification of AI-related **skills** and **capabilities** within the banks, and areas in need of development per the Enhanced Competency Framework on Fintech and Regtech Skills Framework published by the HKMA. Define roles and responsibilities of **people** involved in the AI development lifecycle, for example, who should be responsible for continuous monitoring of the AI solutions and subsequent refinement of the underlying models.

- The key **processes** and templates, for example, a process map detailing the steps and actors involved in conducting AI model evaluation, along with the standardised model evaluation form to document the evaluation.

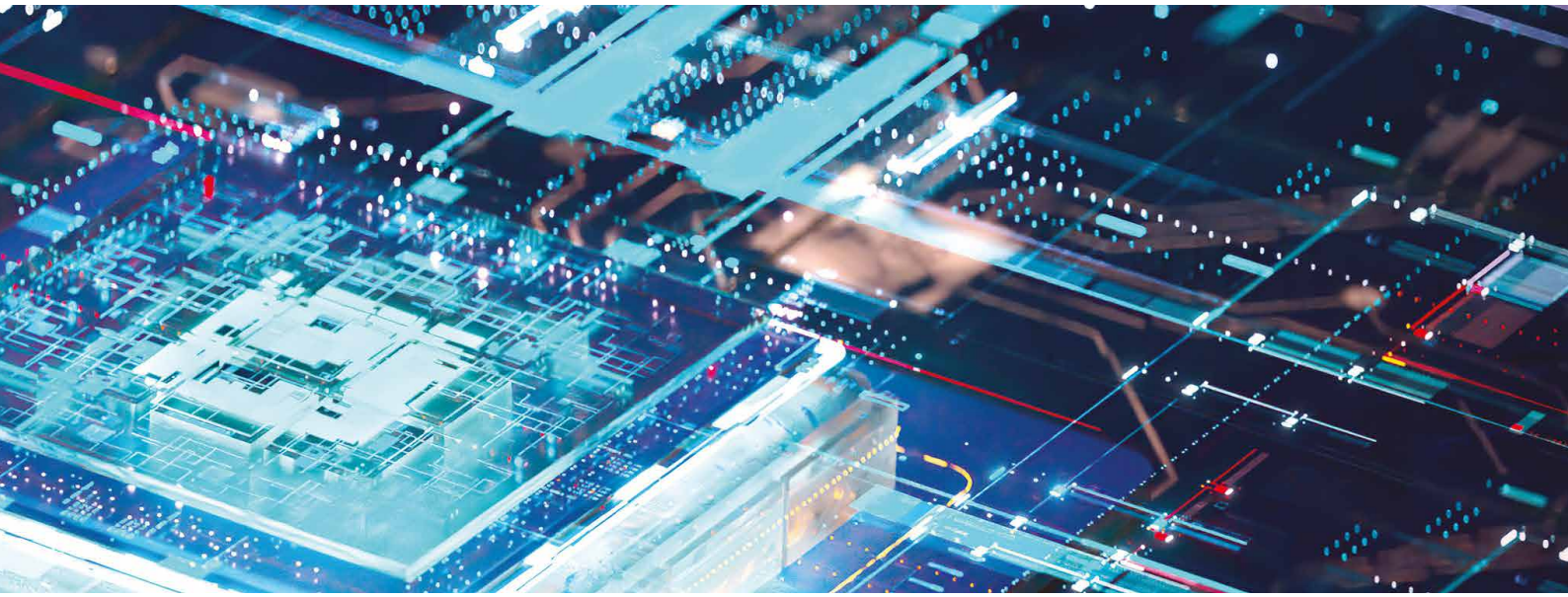
- The **technology** available to support the key processes, and data integration considerations to enable the adoption of AI-based solutions.

- **Governance** and guidelines, **data governance** framework, and determining a **service delivery model** to ensure that there are clear company policies and procedures around the adoption of AI-based solutions.

Establish governance committees: Targeted AI governance committees ensure the right decision-makers come together to make informed decisions to steer the development and use of AI and address the unique risks and issues of AI-based solutions.

Build a risk management framework: A bank should consider implementing an AI-specific risk management framework to facilitate the monitoring, identification, and prioritisation of AI-solution risks. The framework should contain risk mitigation strategies covering the AI solution development lifecycle, for example system failure, ethical concerns, and cybersecurity.

Continuous control: A bank should maintain continuous control over the AI-based solution post-implementation. Necessary capabilities and skillsets within the bank should be acquired or developed to enable the continuous governance and risk management of AI-based solutions. Regular audits of AI-based solutions also need to be put in place to identify risks and ensure compliance with local regulations.



3.3 AI-based Regtech solution implementation

When adopting an AI-based Regtech solution, a bank should follow a standardised project implementation approach. The previous research showed that 61% of surveyed Hong Kong banks partner with a third-party vendor to implement Regtech solutions, with 8% using purely in-house development capabilities. Figure 2 below is an example of a standard project implementation approach that a bank can consider when partnering with third parties to adopt AI-based Regtech solutions.

Figure 2: Sample standard project implementation approach

Source: KPMG

1. Strategy (Initiate)

It is important to align the objectives and target outcomes of AI-based Regtech solutions with the organisation's vision and strategy. After the objectives are defined, the project team should understand the organisational AI capabilities and AI governance to make the buy-or-develop decision, define the project scope, and define roles and responsibilities. These steps ensure a proper foundation for an AI project and help to avoid future deviations from the project goal.

2. Design

The second phase aims to understand how to design the solution within an organisation's operating model. This involves:

- Review the data governance framework, including a detailed technical review of data quality, data lineage, and the defined schema/template. Work with the vendors to identify raw data sources, conduct data cleansing, and data preparation work.
- Evaluate the process surrounding the Regtech solution to identify process re-design and re-engineering opportunities. It should be noted that implementing a large number of point solutions from different vendors can add unnecessary complexity and cause implementation and maintenance issues.
- Assess if the organisation has the right level of knowledge, skills and technology to maintain and conduct a continuous evaluation of the AI models post implementation.
- Work with the vendors to modify the AI solution to meet relevant business or regulatory requirements.

This is a phase that requires extensive discussion and communication. All design decisions must be properly documented to ensure the solution will be built and tested based on the specifications.

3. Model (Build)

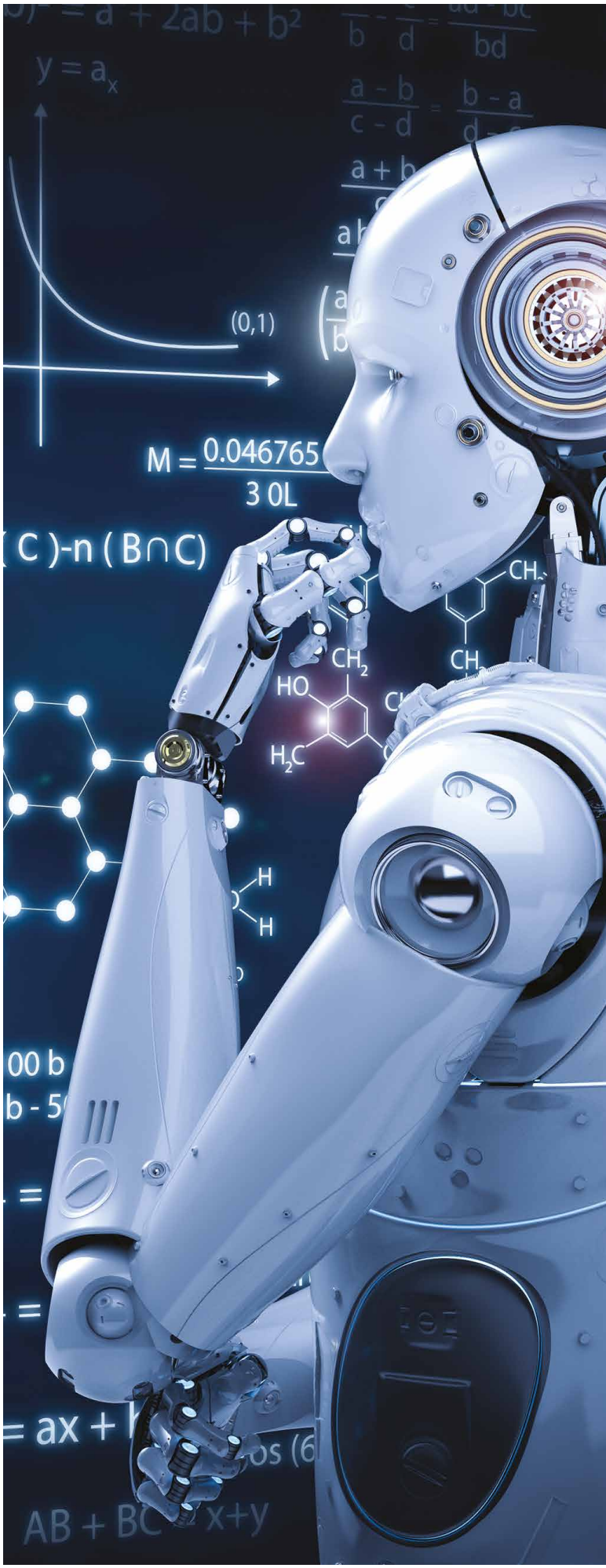
During this phase, the AI models will be built/trained. The steps include domain classification, intent classification, manual labelling, trained recognition, and word vector clustering. The team should evaluate the model training methodology and procedures in accordance with the AI governance framework, including a compliance check of the solution with internal policies, business requirements, and regulations.

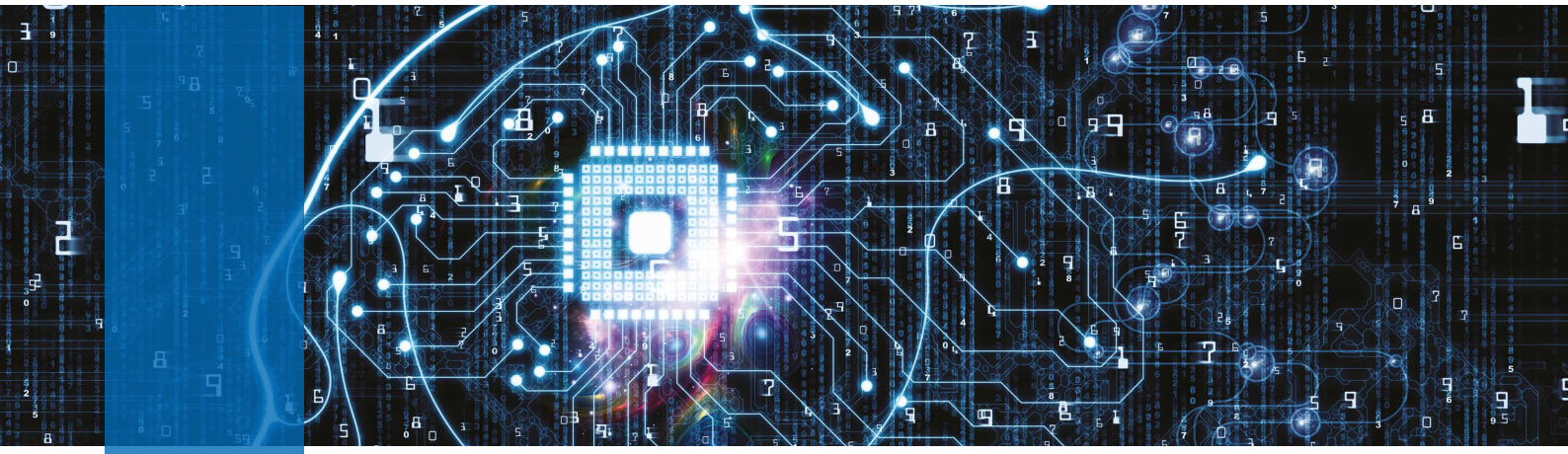
4. Evaluate (Testing)

The next phase involves quality control model experiments to evaluate the solution using test data to measure accuracy and precision and cyber-security related testing to uncover potential vulnerabilities. The test result should undergo stakeholder review, technology review, subject matter expert evaluation, and appropriate acceptance process. The outcome of this phase should be a decision on the suitability of the solution.

5. Deploy and Evolve

The implementation of the solution should follow the defined implementation plan and include a post-implementation review period to capture requirement changes and improvement opportunities. The solution implemented should be continuously monitored for performance, supported for incident response and allow for user feedback.





04 Regtech use cases

Various AI-based Regtech solutions have been developed or adopted by banks. Two use cases and their key learning points are summarised below.

4.1 Use Case #1 – Automated supervision of financial product sales process against regulatory requirements

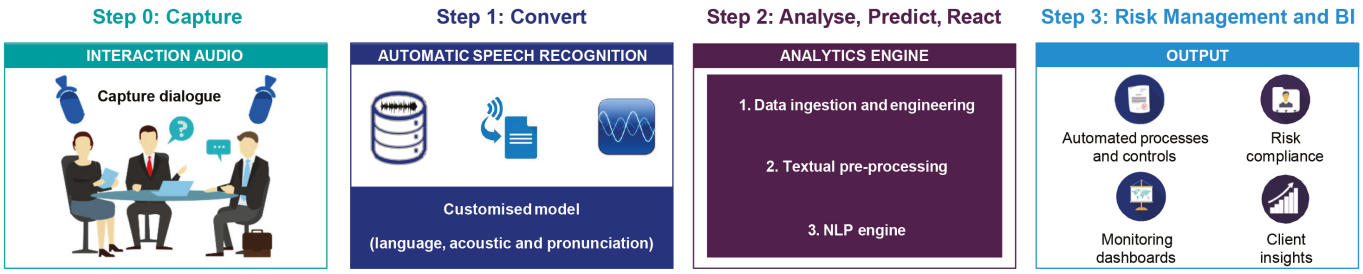
4.1.1 Challenge

One of the largest global private and investment banks reported a lack of coverage and inefficiencies in reviewing calls between Relationship Managers (RM) and customers. The RM often forgot to ask for key client information during the call, making it difficult to determine compliance with suitability or disclosure requirements. Moreover, the management was unclear about the trade status, while operation and compliance teams spent considerable time on manual documentation and reviews.

4.1.2 Solution and benefits

The bank deployed a customer interaction analytics tool powered by AI technology to streamline operation and assist RM in identifying missing client information during the sales process to maximise compliance. As illustrated in Figure 3 below, step 0 of the solution was to capture the audio of regulated product order taking between an RM and customer. The audio was then converted to text via automated speech recognition and speech-to-text technology. Once converted, the machine-readable text was analysed via textual pre-processing that cleaned the text (such as removal of stop words), followed by the use of an NLP engine for iterative analysis. Missing client details and risk compliance status were displayed in near real-time on the screen to alert the RM for their actions before ending the call. In addition, the tool generated ad-hoc and regular alert reports for the compliance and operation staff to review and identify data-driven insights.

Figure 3: Illustration of the customer interaction analytics tool



By automating the voice call monitoring and analysis, the bank was able to gain the following benefits:

- **Enhanced risk management:** The near real-time automated compliance reports enabled real-time self-compliance by the RM against a pre-defined set of business and regulatory rules. This tool also made it possible to monitor compliance at an aggregated level, allowing risk management teams to identify and remediate any potential breaches.

- **Operational efficiency:** The tool enabled the automation of the compliance check process. Previously the bank could only conduct sample checks on recorded conversations. However, the tool can now monitor all conversations with the issuance of exception reports for manual follow up.

- **Business intelligence:** After the audio was transcribed, the tool could then apply data aggregation and keyword analytics to uncover conversational insights. For example, team managers can use the tool to identify customer call trends. The tool could also perform root cause analysis that was used to improve products and services and identify training and development areas.

4.1.3 Key success factors

The bank did not have sufficient experience or internal capabilities for developing AI-based solutions. In this case, it looked for a technology partner with an existing proven and scalable solution to shorten the time-to-market.

- The AI-based solution was implemented in three months as a **Proof of Concept** (PoC) covering one language type (English) and one functional area (mis-selling of products). The PoC allowed the bank to experience the benefits of adopting the AI-based Regtech solution and validate the outputs against existing processes, thereby, minimising accuracy and reliability-related risks. The solution was also scalable, which allowed future extension of use cases in the sales area such as product disclosure coverage.

- In collaboration with the Regtech solution vendor, the bank also engaged an external consultant that brought in an approach and best practices to build an **AI governance framework**. The consultant team also contributed local regulatory and compliance subject matter expert knowledge, through which the bank was able to gain capabilities to start developing its own AI governance and risk management frameworks to facilitate the adoption of future AI solutions.

4.2 Use Case #2 – Federated Learning technology to enable bankruptcy detection

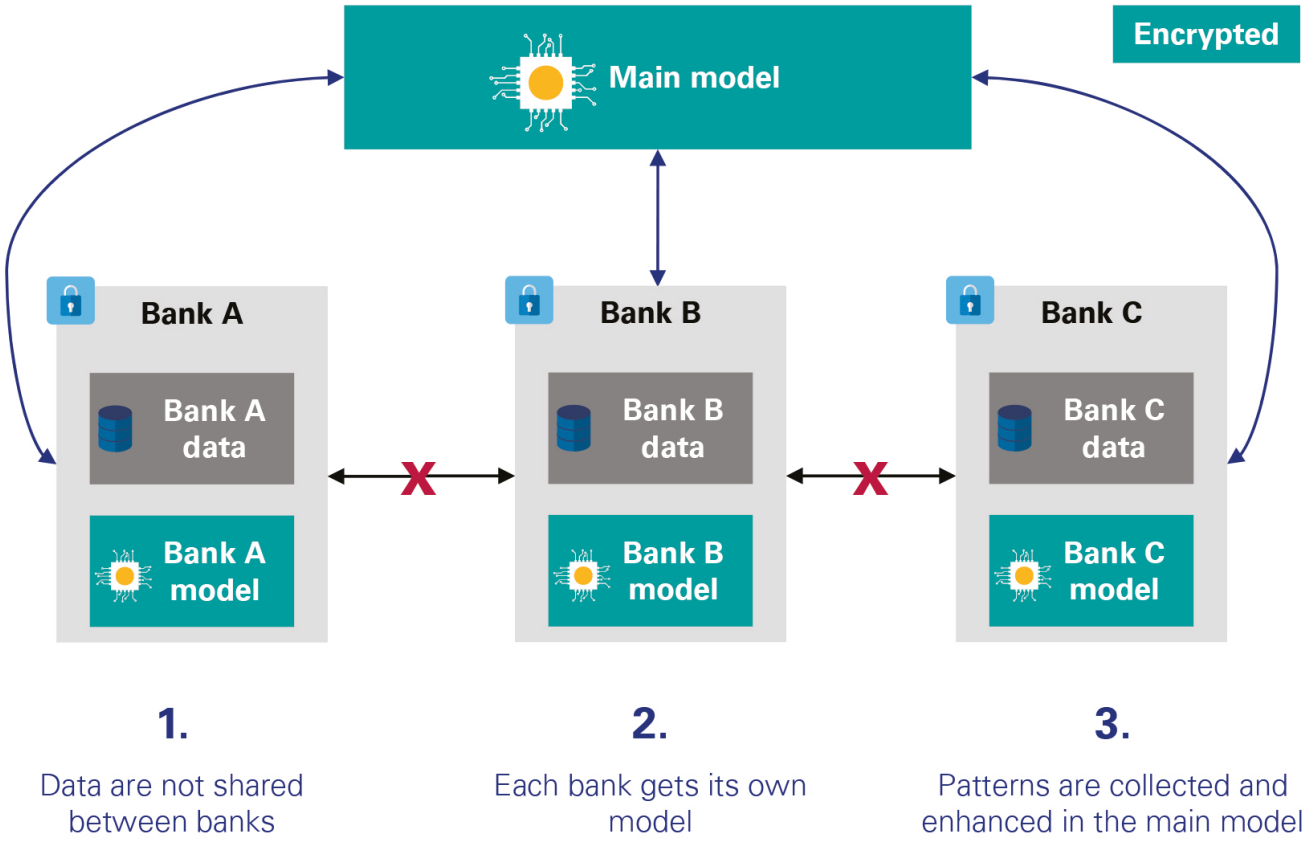
4.2.1 Challenge

To continuously monitor and predict the repayment ability of corporate loan customers, operational teams within a commercial bank traditionally needed to gather and review a large amount of paperwork from customers and perform manual vetting. Such a process to predict potential customer bankruptcy and customers' inability to pay back loans was inefficient and increased the loan-default risk mitigation control effort for the bank. Before the bank could adopt an AI-based Regtech solution to automate the bankruptcy prediction process and increase its predictive capability, a holistic and complete dataset of its customers was required. Moreover, the bank was concerned about risks such as data loss and data privacy. As such, the bank was reluctant to share data with fellow banks or third-party Regtech vendors to develop a Regtech solution.

4.2.2 Solution and benefits

A PoC using Federated Learning technology to identify bankruptcy risks was initiated by Hong Kong Science Park[12] to address the above data-related challenges. A Federated Learning Network platform was developed and three banks participated in the PoC (illustration provided in Figure 4). With the Federated Learning platform, data was not shared between banks, and each bank got a model to train locally using its own data. Patterns derived from each model were then collected and enhanced in the main model.

Figure 4: Illustration of the Federated Learning network platform



[12] HKSTP unveils FinTech Virtual Lab to accelerate FinTech R&D and commercialization, Hong Kong Science and Technology Park, https://www.hkstp.org/press-room/hkstp-unveils-fintech-virtual-lab-to-accelerate-fintech-rd-and-commercialisation/

Benefits from using Federated Learning to identify bankruptcy risks included:

- **Sharing insights without sharing data:** Training machine learning models requires a large amount of data. It is often difficult for a bank or a Regtech solution vendor to gain access to a comprehensive set of data to develop accurate models for specific risk management areas such as loan-default risks. The Federated Learning Network platform offered a secure environment for the three participating banks to collaborate and build a machine learning model together, without disclosing their own data to each other. This secure design greatly shortened the number of internal risk reviews and approvals the banks required to develop the machine learning model.

- **Enhanced risk management:** The Federated Learning Network platform enabled multiple data vendors to build collaborative machine learning models while safeguarding data privacy, hence empowering more holistic monitoring of corporate loans and accurate prediction of client bankruptcy risks as compared to the existing reactive manual processes.

4.2.3 Key success factors

- **Clear guidelines on data and AI usage:** The banks followed the relevant guidelines and principles on AI usage of data and sought the necessary internal approvals to participate in the PoC.

- **Skills and capabilities:** The Federated Learning PoC involved business and technical experts with various skills and capabilities for successful collaboration. Firstly, data specialists within each bank ensured the required data were available and of good quality. Data scientists and machine learning specialists then trained and continuously retrained the model and validated outputs. Lastly, domain subject matter experts in the loan-default risk management area provided business input and validated the outcomes, while IT teams handled the integration requirements.

The above two use cases illustrate how banks in Hong Kong are leveraging AI-based Regtech solutions. Both use cases adopted AI technology to enhance compliance and risk management capabilities to produce more traceable, sustainable, and consistent outputs. The above use cases clearly demonstrate that successful AI adoption requires banks to ensure proper risk management measures are put in place by establishing proper data governance and AI governance frameworks.

A Appendix

A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Paul McSheaffrey, James O'Callaghan, Stanley Sum, Angela Zhang, Wingki Lam, Kelly, editor Philip Wiggenraad

A.2 Relevant regulatory requirements and/or guidance

Name	Link
Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf
High-level Principles on Artificial Intelligence	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf
Guidance on the Ethical Development and Use of Artificial Intelligence	https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf
Reshaping Banking with Artificial Intelligence	https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_on_AI.pdf
Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf
Artificial Intelligence in Banking: the changing landscape in compliance and supervision	https://www.aof.org.hk/docs/default-source/hkimr/applied-research-report/airep.pdf