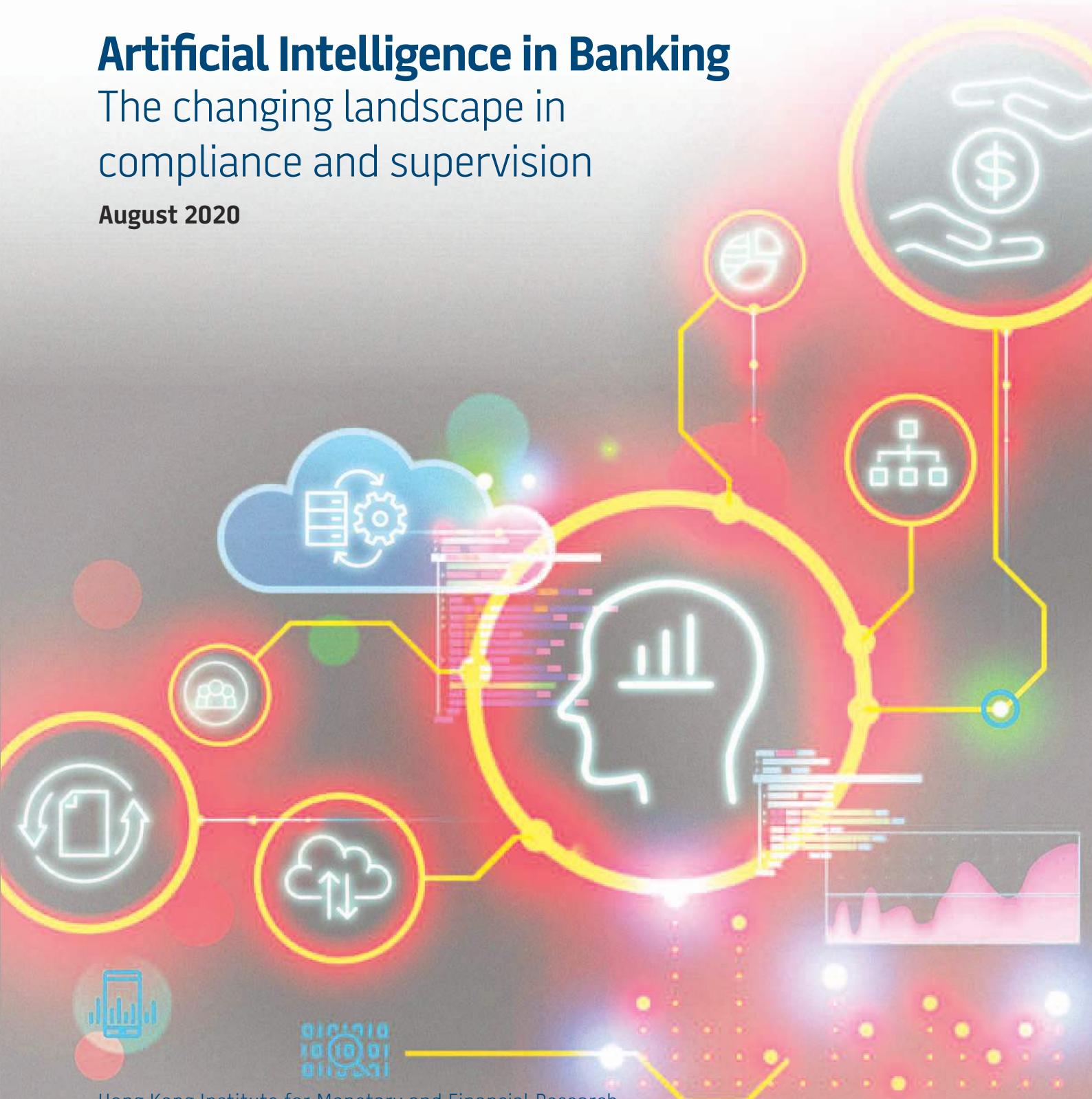


# Artificial Intelligence in Banking

## The changing landscape in compliance and supervision

August 2020



# CONTENTS

---

	Page
<b>Foreword</b>	<b>2</b>
<b>Acknowledgements</b>	<b>3</b>
<b>Executive Summary</b>	<b>4</b>
<b>1. The New Age of Artificial Intelligence in Hong Kong's Banking Industry</b> Opportunities, risks and challenges	<b>6</b>
<b>2. Bank Governance and the Use of Artificial Intelligence</b> Why should banks care about AI risks, and how to manage them?	<b>14</b>
<b>3. Oversight of Artificial Intelligence in Banking — A Complex Task</b> Policy responses, strategies and challenges	<b>35</b>
<b>4. AI-aided Compliance and Supervision</b> How will Regtech and Suptech change the landscape of compliance and banking supervision?	<b>50</b>
<b>Conclusions</b>	<b>60</b>
<b>Appendix A: Background of the HKMA AI Survey</b>	<b>61</b>
<b>Appendix B: References</b>	<b>62</b>

# FOREWORD

2

The application of artificial intelligence (AI) in banking has advanced to a new level, thanks to maturing techniques in big data analytics and machine learning, as well as enhancements in computational power. In Hong Kong, the use of AI in the banking industry is expanding to cover key functional areas including front-line businesses, risk management and back office operations. These new technologies are increasingly used to perform more sophisticated tasks such as credit assessments and fraud detection. They also enable banks to better serve their customers, providing the convenience of remote onboarding for account opening and enquiry handling using client-facing chatbots.

In an earlier report titled *Reshaping Banking with Artificial Intelligence* released by the Hong Kong Monetary Authority in December 2019, we shared a number of use cases and potential applications to illustrate how banks can integrate AI into their business models, and discussed the implementation issues in AI adoption. In this report, we highlight the opportunities and challenges from the broader use of the technology by banks in Hong Kong. At the same time, we emphasise the importance of managing the risks arising from AI adoption that relate to data quality and privacy, complexity of understanding and validating AI models, and new cyber threats to AI applications.

The more extensive use of AI in banking will also present new opportunities and challenges to regulators seeking to safeguard financial stability while enhancing consumer protection and nurturing innovation. The landscape of compliance and supervision for the banking sector is likely to evolve with more widespread adoption of AI. The technology can be harnessed to streamline the compliance process, introduce machine-readable regulations and automate data collection for supervisory purposes. Additional insights may also be generated from various types of data collected from banks.

The prospects for a broader and more advanced use of AI in banking, compliance and supervision appear promising, encouraged by gains in efficiency and enhancement in risk management. Policymakers are exploring further use of AI in improving compliance (Regtech) and supervisory capacity (Suptech), which is mutually beneficial to banks and regulators.

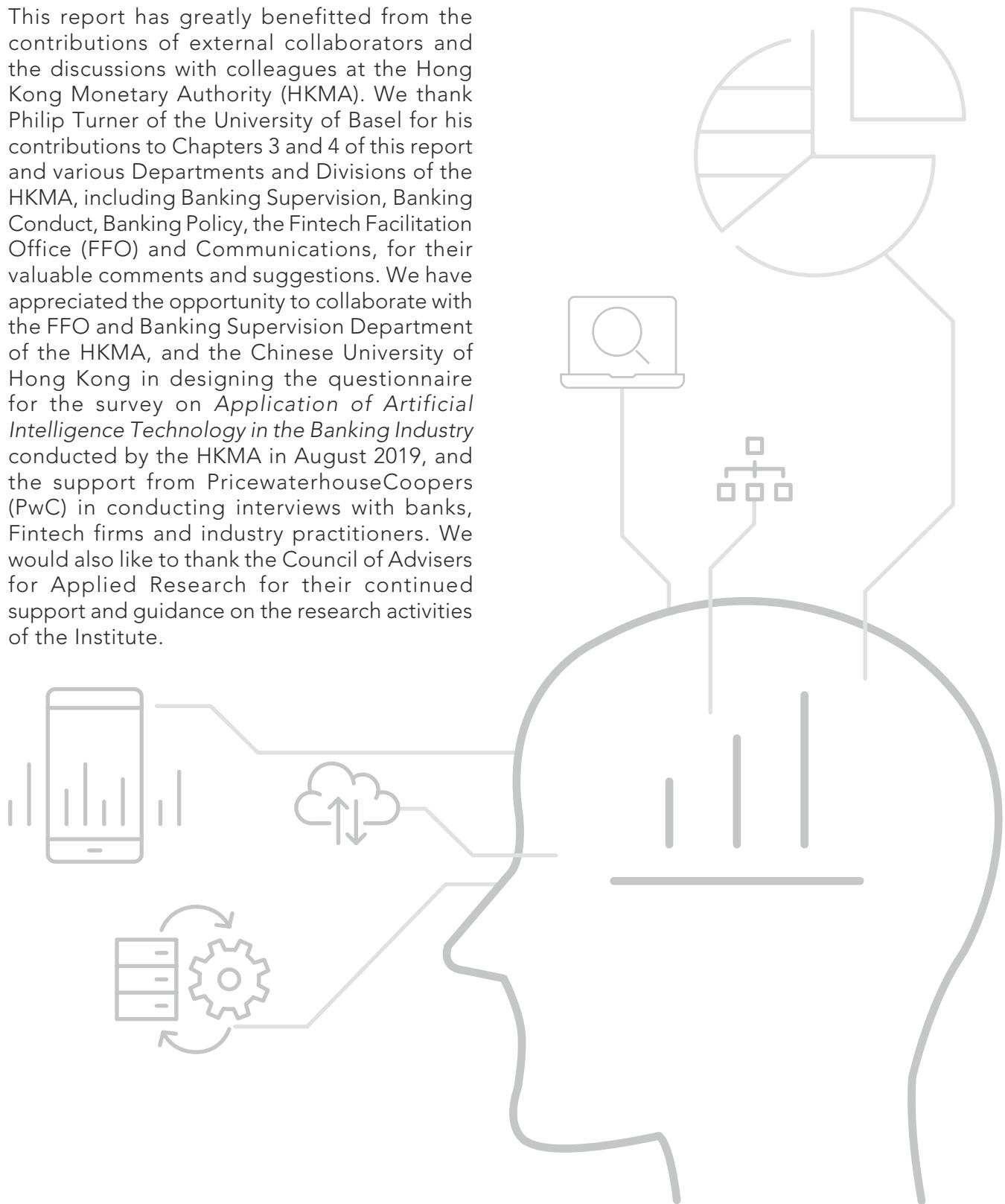
We hope that this report serves as a useful starting point towards understanding the broad implications of AI adoption for the banking industry, as well as its compliance and supervision.

**Mr. Edmond Lau**  
Senior Executive Director  
Hong Kong Monetary Authority

Deputy Chairman  
Hong Kong Institute for Monetary  
and Financial Research

# ACKNOWLEDGEMENTS

This report has greatly benefitted from the contributions of external collaborators and the discussions with colleagues at the Hong Kong Monetary Authority (HKMA). We thank Philip Turner of the University of Basel for his contributions to Chapters 3 and 4 of this report and various Departments and Divisions of the HKMA, including Banking Supervision, Banking Conduct, Banking Policy, the Fintech Facilitation Office (FFO) and Communications, for their valuable comments and suggestions. We have appreciated the opportunity to collaborate with the FFO and Banking Supervision Department of the HKMA, and the Chinese University of Hong Kong in designing the questionnaire for the survey on *Application of Artificial Intelligence Technology in the Banking Industry* conducted by the HKMA in August 2019, and the support from PricewaterhouseCoopers (PwC) in conducting interviews with banks, Fintech firms and industry practitioners. We would also like to thank the Council of Advisers for Applied Research for their continued support and guidance on the research activities of the Institute.



# EXECUTIVE SUMMARY

4

**The trend of increasing use of AI in banking is clear. Banks in Hong Kong have been integrating the technology into various key functional areas** including front-line businesses, risk management, back office operations and customer services. According to a survey conducted by the HKMA in August 2019, over 80% of the participating banks view AI adoption as a way of reducing operating costs, improving efficiency and strengthening risk management. Reflecting optimism about the prospects of broader AI adoption, some 80% of the banks plan to increase investment in the technology over the next five years.

**The broader use of AI will create new opportunities, but also pose new risks and challenges to banks**, including the lack of quality data and data protection, and difficulty in explaining and validating AI models. Banks participating in the survey are aware of these risks and they have regular reviews to identify AI risks (68% of AI-utilising banks) and clear procedures to address model defects (70%). Banks in Hong Kong also highlight additional challenges including issues related to development such as shortage of talent, technical aspects such as increased complexity of AI models, and issues associated with the evolving regulatory environment.

**The growing use of AI applications in online and mobile banking may expose banks to new cyber threats.** Banks will need to identify potential weaknesses in their cyber defence systems by conducting regular tests, and assess the resilience of their AI applications to more sophisticated cyberattacks. Strengthening the cybersecurity of the most important and vulnerable operations of banks and enhancing the security features of cloud computing will become increasingly important.

**Following industry good practices can mitigate the risks arising from a broader adoption of AI.** A robust governance framework requires effective monitoring of three key aspects of AI model risks including data inputs, model design and validation. On data inputs, a data governance framework is useful in mitigating the risk of data breaches or data flaws. On model design and validation, an enhanced model-risk management framework incorporating big data analytics and machine learning techniques is important in understanding model design and validating model outcomes.

**In supervising the adoption of AI by banks, regulators seek to balance the objectives of maintaining financial stability, upholding consumer protection and nurturing innovation.** With this in mind, bank regulators around the world have generally adopted the strategy of setting out guiding principles to promote a sound, fair, ethical and transparent use of AI technologies. In line with this practice, the policy of the HKMA on AI adoption is to apply the twin principles of technology neutrality and risk-based supervision. Three sets of supervisory guidelines or initiatives have been implemented to govern the prudent use of data analytics and AI models, and to strengthen the resilience of cybersecurity systems.

**The more extensive use of AI by banks suggests that regulators may develop new thinking when monitoring and assessing risks to financial stability.** From a micro perspective, the greater use of machine learning techniques to train algorithms on larger and more diverse data sets presents new complexities for bank supervisors. Regulators need to equip themselves with knowledge on data science and programming. From a systemic perspective, the increased interconnectedness and competition between banks and Big Tech firms, as well as the potential risks of increased market concentration and contagion, warrant ongoing monitoring of the impact of AI adoption on financial stability.

**Digitalisation and new AI technologies will lead to profound changes in the landscape of compliance and supervision.** Banks and regulators are exploring the use of AI to streamline the compliance procedure and integrate the technology into the supervisory process. Currently, the application of AI by banks in compliance, or Regtech, is mainly for automation in regulatory reporting and fraud detection. Regulators are also using AI to enhance their supervisory capacity (Suptech). New initiatives include introducing machine-readable regulations and automation in data collection from banks for obtaining new insights or detecting irregular activities. To explore the better use of Regtech and Suptech, the HKMA has launched a number of new initiatives to facilitate developments in these two important areas.

**The prospects for greater use of AI by banks is promising, encouraged by gains in efficiency and enhancement in competitiveness.** Policymakers can play a role in strengthening public-private co-operation and promote knowledge exchange, experience sharing and talent development through organising forums where Fintech companies, data specialists and universities can interact.

# CHAPTER 1

## THE NEW AGE OF ARTIFICIAL INTELLIGENCE IN HONG KONG'S BANKING INDUSTRY

### OPPORTUNITIES, RISKS AND CHALLENGES

- 1.1: Banks are embracing AI on all business fronts
- 1.2: Benefits and opportunities
- 1.3: Risk and governance
- 1.4: Prospects and challenges

Machine Learning  
Big Data  
Models

AML

Automation

# 1 THE NEW AGE OF ARTIFICIAL INTELLIGENCE IN HONG KONG'S BANKING INDUSTRY

## OPPORTUNITIES, RISKS AND CHALLENGES

### HIGHLIGHTS:

- According to a survey conducted by the HKMA in August 2019, the application of artificial intelligence (AI) in the Hong Kong banking industry has broadened to cover key functional areas including front-line businesses, risk management, back office operations and customer services.
- Survey findings show that banks in Hong Kong are optimistic about the prospects of wider adoption of AI as the technology helps reduce operating costs, improve efficiency and enhance risk management.
- The banks participating in the survey are aware of the risks arising from the broader use of AI relating to data quality and privacy, difficulty in explaining and validating AI models, and new cyber threats to AI systems.
- The survey highlights a number of challenges faced by banks in expanding the use of AI. Shortage of talent is a prime concern in developing new AI applications. Technical issues including complexity of AI models and the lack of quality data are important issues to be addressed. On the regulatory front, banks need to adjust their governance policies to align with the evolving regulatory environment.

### 1.1: BANKS ARE EMBRACING AI ON ALL BUSINESS FRONTS

The application of AI technologies in banking has been growing and broadening. On a global scale, a survey conducted with financial institutions by OpenText Corporation shows that about 80% of respondents recognised the potential benefits of using AI applications in businesses.<sup>1</sup> In order to understand the engagement of banks in Hong Kong with AI technologies, the HKMA conducted a survey on *Application of Artificial Intelligence Technology in the Banking Industry* (hereinafter HKMA AI Survey) in August 2019.<sup>2</sup> One of the key results of the survey, summarised in the report *Reshaping Banking with Artificial Intelligence*

released by the HKMA in December 2019, is that the use of AI technologies has become an integral part of banking in Hong Kong. In particular, 89% of retail banks participating in the survey have adopted or plan to adopt AI applications in their businesses.<sup>3</sup>

This chapter complements the analysis reported in the earlier HKMA report on *Reshaping Banking with Artificial Intelligence* and further explores the results of the HKMA AI Survey with the aim of understanding important trends of AI adoption in the Hong Kong banking industry. More specifically, the focus of the discussion is on banks' views of the opportunities and risks arising from AI adoptions and the governance practices put in place.

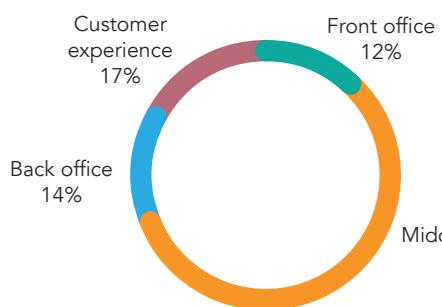
<sup>1</sup> For details, please refer to the report *AI in Financial Services: Next Steps to Realising the Potential*, OpenText Corporation, April 2018.

<sup>2</sup> The survey covers 168 authorised institutions in Hong Kong. Details on the composition of responding banks can be found in Appendix A. Unless otherwise specified, figures quoted in this chapter refer to the survey findings.

<sup>3</sup> AI generally refers to technologies that mimic human intelligence so that they can learn, sense, think and act in order to achieve automation and gain analytic insights. For details on the spectrum of AI applications used in banking, please refer to *Reshaping Banking with Artificial Intelligence*, HKMA, December 2019.

The overall picture that the HKMA AI Survey portrays is encouraging. In fact, both retail and non-retail banks in Hong Kong are found to have broadened the adoption of AI in their key functional areas including front-line businesses, risk management (middle office), back office operations and customer services.<sup>4</sup> The most extensive use of AI applications can be seen in the middle office functions, accounting for some 57% of total number of use cases where the technology has been adopted or planned to be launched.<sup>5</sup> This is followed by customer services accounting for 17%, while front and back offices account for 12% and 14% respectively (Chart 1.1).<sup>6</sup>

**Chart 1.1: Number of AI use cases by functional area of banks  
(% share)**



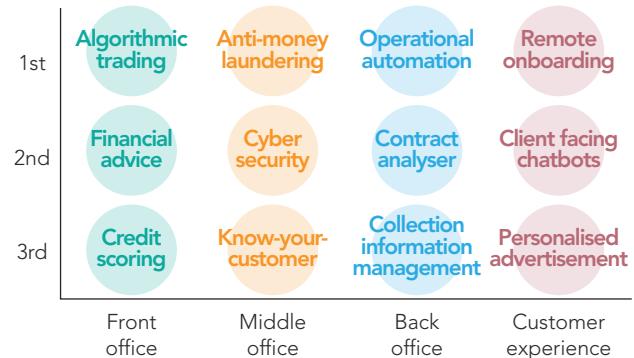
Sources: HKIMR staff calculations based on the HKMA AI Survey.

The most commonly used AI applications in performing middle office functions are anti-money laundering (AML), cybersecurity and know-your-customer (KYC) due diligence (Chart 1.2). Interviews with industry practitioners reveal that AI applications empowered by machine learning (ML) are powerful tools for identifying

The HKMA AI Survey shows that the most commonly used AI applications are risk management tools such as anti-money laundering, cybersecurity and know-your-customer due diligence.

suspicious cases of money laundering based on transaction patterns and customer profiles. This helps reduce the number of false alarms and allows for more focused investigations on the identified cases. In Hong Kong, banks are also using AI and ML to monitor activities on their internet platforms to identify possible cyber threats, taking remedial action as necessary.

**Chart 1.2: Most common AI use cases by functional area  
(top three categories)**



Sources: HKIMR staff calculations based on the HKMA AI Survey.

<sup>4</sup> Front-line business refers to client-facing activities that generate revenue such as lending and treasury operations. Middle office mainly performs the functions of risk control, governance and compliance. Back office mainly includes administrative and support services such as settlements, clearances and accounting.

<sup>5</sup> The survey identifies 51 categories of AI use cases that have been adopted or plan to be launched by banks in Hong Kong. The share is calculated based on the number of use cases reported in the survey by functional area.

<sup>6</sup> The percentage share only reflects the number of AI use cases in a particular functional area instead of contribution to value-added of banks.

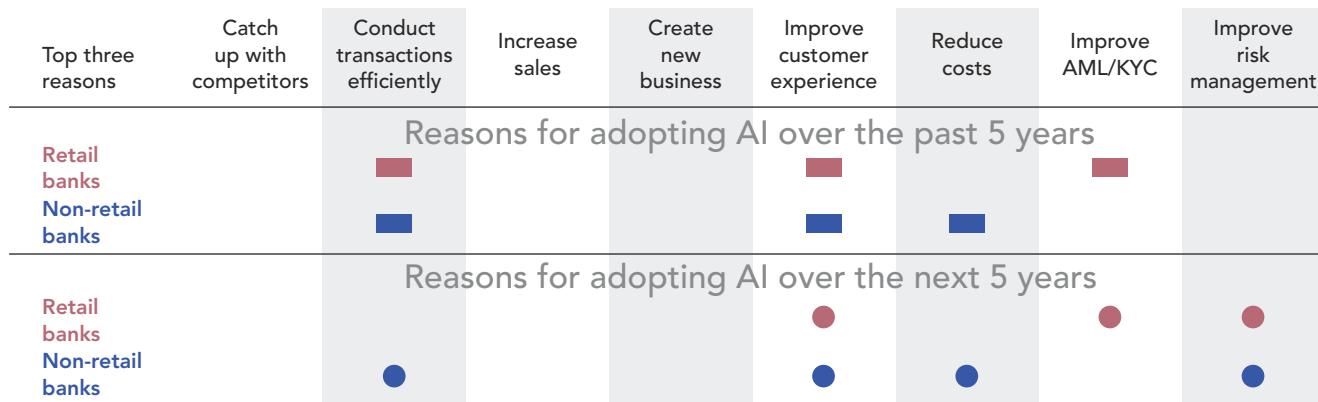
Front office functions that are performed with the aid of AI by banks participating in the survey include algorithmic trading, financial advisory services and credit scoring. To save on operating costs and reduce human error, banks are also using AI to automate back office operations including preparing routine reports, analysing contracts and managing information on debt collection.

It is also common for banks to use AI to improve customer experiences. The survey results show that most of the retail banks in Hong Kong have used remote on-boarding to better serve their customers such as opening accounts using electronic means. Other AI applications include using chatbots to handle customer enquiries and personalised advertisements to improve communications with their clients.

## 1.2: BENEFITS AND OPPORTUNITIES

According to the HKMA AI Survey, banks in Hong Kong recognise the benefits of adopting AI. Table 1.1 summarises the major reasons for banks adopting AI. It shows that over the past five years, both retail and non-retail banks used the technology to improve customer experience and enhance transaction efficiencies. Retail banks also used AI to strengthen AML surveillance and KYC due diligence. For non-retail banks, an additional motivation for using AI is to reduce operating costs through automation.

**Table 1.1: Major reasons for adopting AI**



Note: Both "Conduct transactions efficiently" and "Reduce costs" are ranked the third most popular reason by non-retail banks for adopting AI over the next 5 years.

Sources: HKIMR staff calculations based on the HKMA AI Survey.

In the HKMA AI Survey, banks were asked to indicate three major reasons for adopting AI over the next 5 years. Both retail and non-retail banks state enhancing risk management and improving customer experience as the key drivers for greater use of AI in future. For retail banks, they also rate strengthening AML surveillance and KYC due diligence as one of the main reasons for applying AI. Meanwhile, non-retail banks continue to see that the technology as helping to achieve cost reductions or efficiency gains.

The majority of survey respondents state that their objectives of using AI have been accomplished to a large extent. Over 80% of retail and non-retail banks share the views that AI adoption helps improve efficiency in transactions, strengthen AML surveillance and KYC due diligence and enhance risk management (Table 1.2).

Over 80% of banks participating in the survey view AI adoption as a way of improving efficiency, enhancing risk management and strengthening AML surveillance and KYC due diligence.

**Table 1.2: Banks' objectives accomplished after adopting AI**

(% of respondents)	Retail banks	Non-retail banks
Catch up with competitors	74%	53%
Conduct transactions efficiently	83%	81%
Increase sales	67%	38%
Create new business	61%	44%
Improve customer experience	100%	74%
Reduce costs	89%	78%
Improve AML / KYC	94%	81%
Improve risk management	85%	80%

Sources: HKIMR staff calculations based on the HKMA AI Survey.

### 1.3: RISK AND GOVERNANCE

While AI adoption provides banks with potential benefits and opportunities, it also poses new risks that need to be properly managed. The HKMA AI Survey identifies a number of risks that banks in Hong Kong see as key in governing the prudent use of AI. Retail banks ranked data quality and privacy, model validation and model reliability as the top three major risks and governance issues in using AI applications (Chart 1.3). Data quality and privacy are deemed by retail banks as the most important governance issue. This is understandable as AI models cannot perform well without reliable and relevant data, and high standards of data privacy should be maintained to earn customers' trust. Model validation also plays a pivotal role in verifying that AI models are robust and yield sensible outcomes, while model reliability and interpretability are instrumental in gaining support from management and regulators. Similar to retail banks, non-retail banks also ranked data quality and privacy the top priority in AI governance, followed by model validation, model reliability and meeting compliance standards (Chart 1.4).

Key AI governance risks highlighted by banks participating in the survey include data quality and privacy, model reliability and interpretability, and model validation.

**Chart 1.3: AI governance risks perceived by retail banks**

Note: The size of the circles is proportional to the number of responses.

Sources: HKIMR staff calculations based on the HKMA AI Survey.

**Chart 1.4: AI governance risks perceived by non-retail banks**

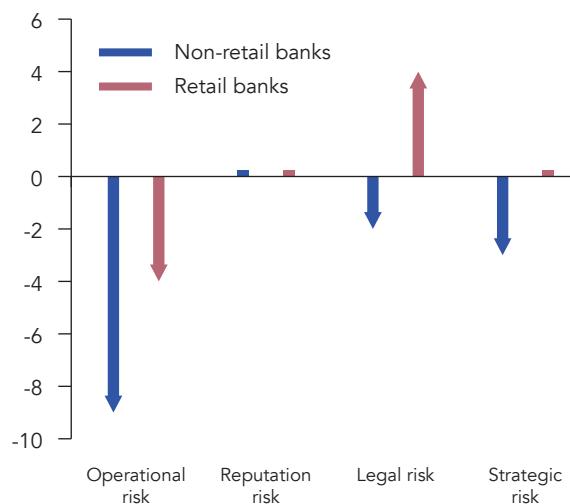
Note: The size of the circles is proportional to the number of responses.

Sources: HKIMR staff calculations based on the HKMA AI Survey.

The broader use of AI applications may also expose banks to additional operational, reputation, legal and strategic risks. In the HKMA AI Survey, retail and non-retail banks provide different assessments of these potential new risks. Some retail banks believe that using AI to replace human input may increase legal risk but will have little impact on reputational and strategic risks (Chart 1.5). Non-retail banks generally believe that AI applications help lower legal and strategic risks, with little impact on bank's reputation. Both retail and non-retail banks see using AI as helping to reduce operational risk through minimising human error.

### Chart 1.5: Impact of AI adoption on banks' risk profile

(score; positive=higher risk)

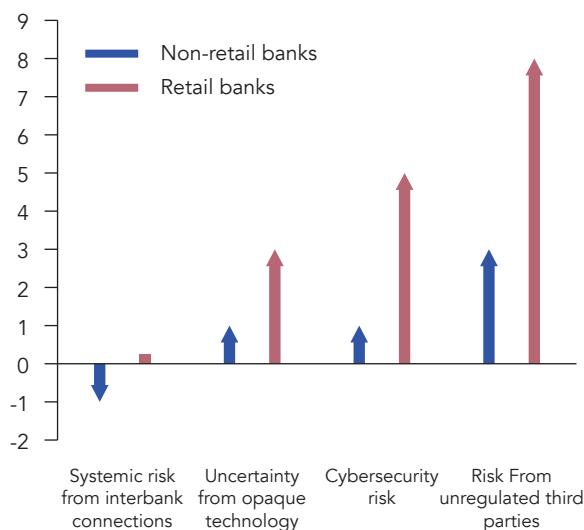


Sources: HKIMR staff calculations based on the HKMA AI Survey.

Banks participating in the survey are also concerned about the uncertainty from using opaque technologies, threats to cybersecurity and the risk from unregulated third parties, such as AI vendors and Big Tech firms (Chart 1.6). Both retail and non-retail banks consider the risk due to unregulated third parties as the most prominent risk when the use of AI is more widespread in Hong Kong. Retail banks also deem cyberattacks to AI systems as an important threat, while non-retail banks are less concerned over the impact of using AI on systemic risks arising from the interbank channel.

### Chart 1.6: Other risk factors of banks adopting AI

(score; positive=higher risk)

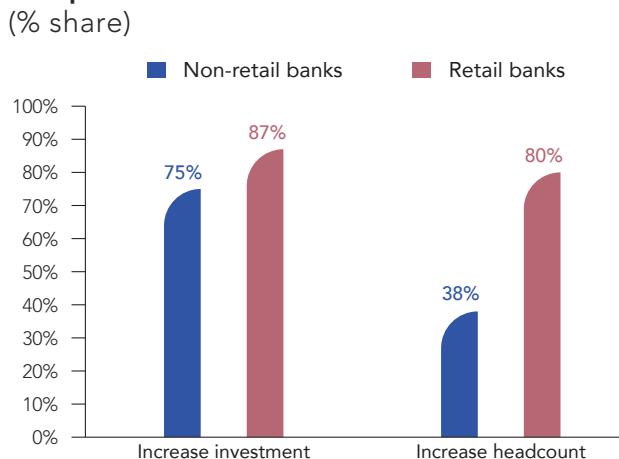


Sources: HKIMR staff calculations based on the HKMA AI Survey.

## 1.4: PROSPECTS AND CHALLENGES

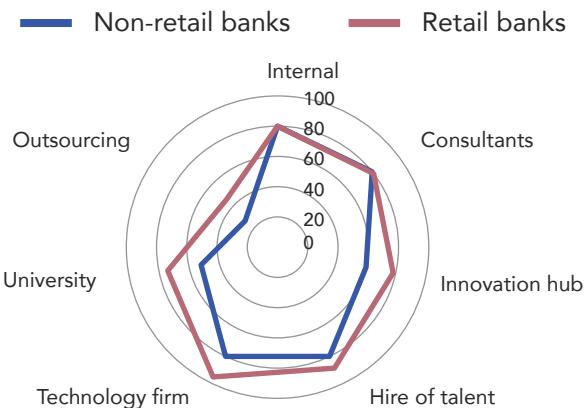
Banks in Hong Kong are optimistic about the prospects of integrating AI into their business plans. According to the HKMA AI Survey, 87% of retail banks and 75% of non-retail banks expect to increase investment in AI technologies over the next five years. In terms of manpower, most banks are planning to employ more people dealing with AI applications (Chart 1.7). In the near future, banks plan to develop AI applications through collaborations with technology or consultancy firms, hiring AI talent and using internal resources (Chart 1.8).

### Chart 1.7: Prospects of investment and manpower in AI



Sources: HKIMR staff calculations based on the HKMA AI Survey.

**Chart 1.8: Methods of developing AI by banks in future**  
(% share)

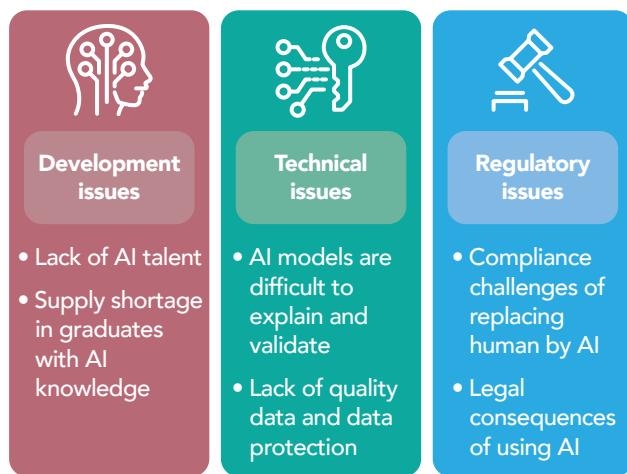


Sources: HKIMR staff calculations based on the HKMA AI Survey.

Banks in Hong Kong are optimistic about the prospects of a broader use of AI, with some 80% of survey respondents planning to increase investment over the next five years.

In order to successfully deploy AI applications, banks participating in the survey have identified three main challenges to overcome in developing applications of AI in Hong Kong. These include development issues such as shortage in AI talent, technical issues such as the lack of quality data and difficulty in explaining and validating AI models, and regulatory issues such as the evolving compliance environment (Table 1.3).

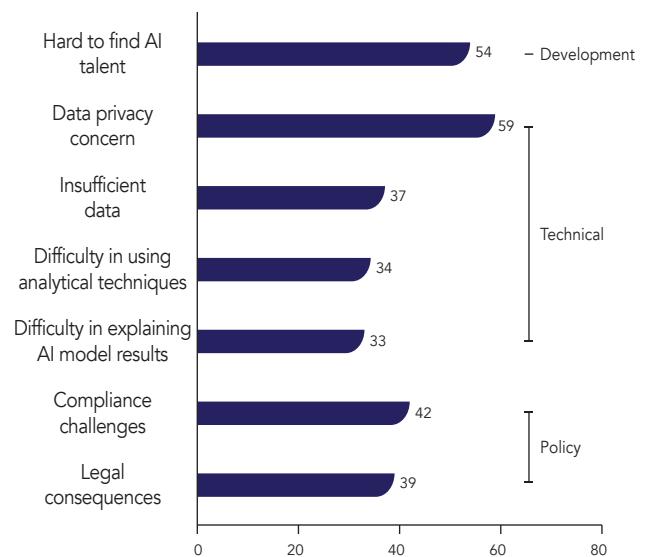
**Table 1.3: Main challenges faced by banks in advancing AI applications**



Sources: HKIMR staff compilation based on the HKMA AI Survey.

On development issues, the HKMA AI Survey shows that 54% of respondents are concerned about the shortage of talent for developing AI applications. On the technical front, data privacy and insufficient quality data are key considerations for banks in developing AI applications, while about one-third of the banks highlight difficulty in using analytical techniques and explaining model outcomes as major challenges in AI adoption. For regulatory issues, some 40% of banks express concerns about replacing human efforts by AI tools, and potential legal consequences with the broader use of AI (Chart 1.9).

**Chart 1.9: Challenges faced by banks in advancing AI development**  
(% share)



Sources: HKIMR staff calculations based on the HKMA AI Survey.

Banks participating in the survey highlight AI talent shortage, data privacy, complexity of using analytical techniques and explaining model outcomes as key challenges for advancing AI development.

# CHAPTER 2

## BANK GOVERNANCE AND THE USE OF ARTIFICIAL INTELLIGENCE

WHY SHOULD BANKS CARE ABOUT AI RISKS, AND HOW TO MANAGE THEM?

- 2.1: Strengthening bank governance for AI adoption
- 2.2: Data governance framework
- 2.3: Machine learning and model-risk management
- 2.4: Cybersecurity of AI systems



## 2 BANK GOVERNANCE AND THE USE OF ARTIFICIAL INTELLIGENCE

WHY SHOULD BANKS CARE ABOUT AI RISKS, AND HOW TO MANAGE THEM?

### HIGHLIGHTS:

- The use of vast amounts of data and machine learning techniques in AI models will likely expose banks to potential risks of data leakage and model design flaws, which may lead to financial losses and undermine banks' reputation.
- Industry good practices in managing AI risks suggest that a robust data governance framework helps mitigate risks of data breaches and data quality issues. Banks also need to integrate machine learning modelling process into existing model-risk management frameworks with rigorous validation procedures and performance tracking.
- It is important for banks, facing new and increasing cyber threats, to identify potential weaknesses in their cyber defence systems and strengthen the resilience of their AI and IT systems to more sophisticated cyberattacks.
- The successful implementation of an AI governance framework requires the alignment of objectives with business goals, as well as good communication with major stakeholders. As there is no one-size-fits-all solution, the management needs to remain flexible and pragmatic in the execution of governance policies.

### 2.1: STRENGTHENING BANK GOVERNANCE FOR AI ADOPTION

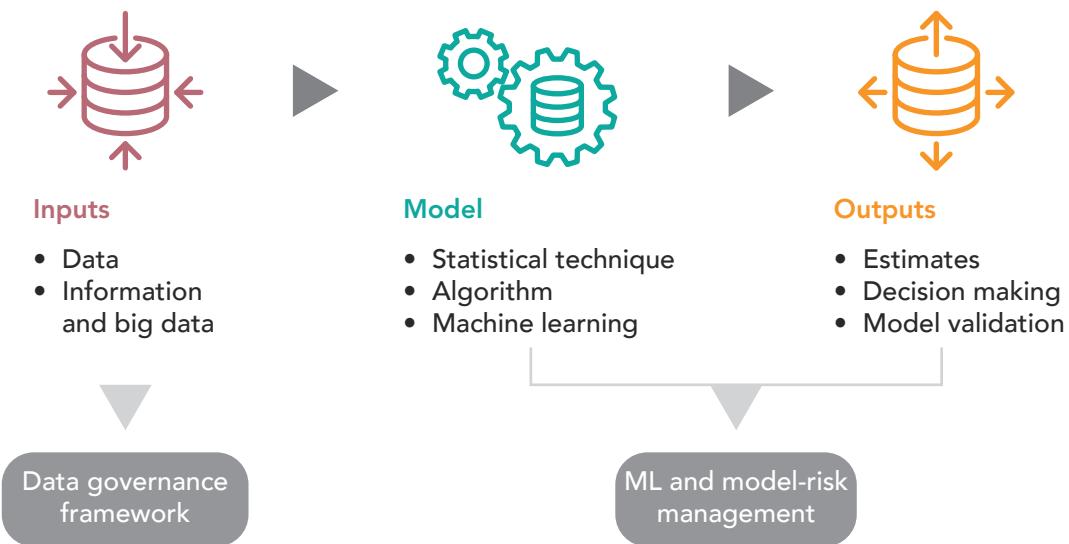
As banks in Hong Kong embrace AI technologies for their businesses, they are also aware of the potential risks from AI adoption related to data quality and privacy, model design and validation issues. It is the responsibility of the management to put in place effective internal control measures to safeguard the prudent use of the technology.

Banks can follow industry good practices to mitigate the risks arising from a broader adoption of AI. A robust governance framework

requires effective monitoring of three key aspects of AI model risks including data inputs, model design and validation (Chart 2.1). Data inputs include structured data and qualitative information from various sources (or big data) that feed into AI models. Model design encompasses assumptions, algorithms and the use of ML techniques in developing decision rules based on data inputs.<sup>7</sup> Model outputs include estimates and outcomes generated from AI models that are subject to verification and validation.

<sup>7</sup> Machine learning is an application of AI that provides IT systems the ability to automatically learn and improve from experience without being explicitly programmed. The process of learning begins with observations or data in order to look for patterns and base its decisions on them.

Chart 2.1: Building Blocks of AI Models and Associated Control Measures



Source: HKIMR staff compilation.

Banks with a broad and intensive use of AI models may need to establish a data governance framework to assure data quality and privacy. Banks also need to strengthen their existing model-risk management systems to ensure the proper use of data analytics and ML techniques in AI models. Depending on the intensity of AI adoption, the scope and scale of data governance and model-risk management could vary across banks. Potential indicators of the intensity of AI adoption may include the extent of reliance on AI models in decision-making, the level of automation and the severity of impact due to defects in model design. Banks with a limited use of data and AI-driven models may integrate data governance and model-risk management functions into existing risk control frameworks, which are then overseen by the risk management or middle office.

## 2.2: DATA GOVERNANCE FRAMEWORK

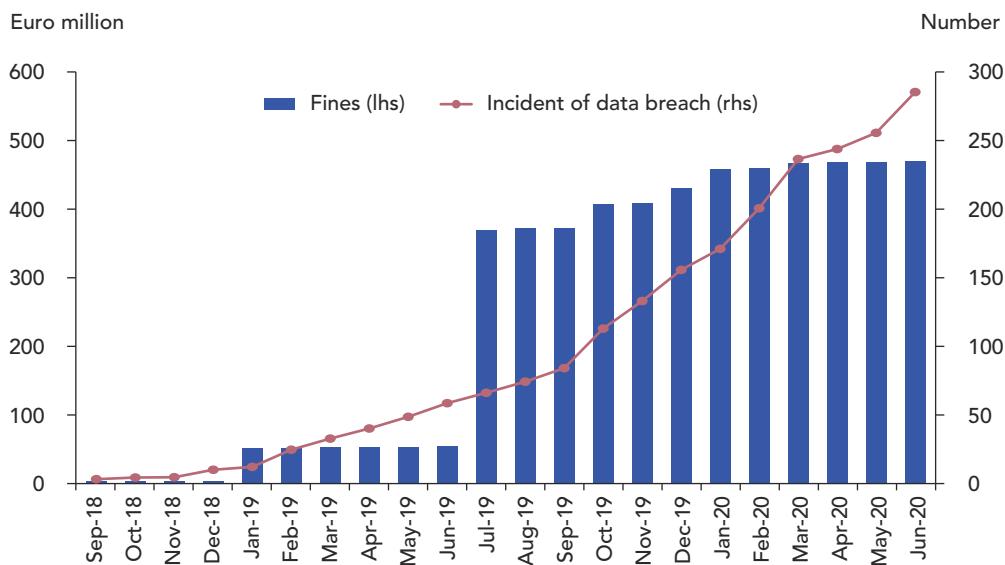
A data governance framework serves two key purposes — to ensure data quality and security. First, **data quality** is of the utmost importance where there is intensive use of big data in AI models for decision-making. In this case, a

centralised data warehouse keeping track of data sources and data accuracy could minimise errors and inconsistency in model outcomes. Second, with the aid of AI technologies, banks can collect and use a large amount of customer data to create new products and provide new services to customers. However, the **data security** risk is high as a breach or leakage of customer data could undermine the integrity and reputation of banks.

Indeed, the consequences of improper use of data could be substantial. According to statistics from the General Data Protection Regulation (GDPR) in Europe, the cumulative fines for data breaches have risen to EUR470 million as of June 2020, with the total number of cases reaching 285 (Chart 2.2). Most data breach incidents relate to insufficient data protection and improper data processing. Some prominent examples include breaches by British Airways, Marriot International and Google in 2019.<sup>8</sup> Outside Europe, a data breach by Equifax in 2017, one of the three largest consumer credit information companies in the US, led to a settlement amount of some US\$700 million in 2019. The increasing number of breaches has raised public awareness of data privacy and prompted more questions about corporate governance in the use and protection of personal data.

<sup>8</sup> According to GDPR, the fines for British Airways, Marriot International and Google Inc were EUR205 million, EUR110 million and EUR 50 million respectively.

**Chart 2.2: Cumulative fines and Incidents Related to Data Breaches Under GDPR**



Source: GDPR Enforcement Tracker.

### 2.2.1: Key elements in a data governance framework

With growing public awareness of data privacy and the increasing use of data in business analytics, data risk management and security have become an integral part of corporate governance. Data specialists, IT firms and universities have advocated several good practices in governing the proper use and protection of data. Based on corporate needs and the intensity of data used by banks, a data governance framework could comprise the following components:<sup>9</sup>

- **Objective and policy:** This aspect is mainly the responsibility of the management, which includes reviewing existing data-related policy and reaching consensus with major stakeholders such as IT, the risk control office and business units. After detailing the operating procedures, the data governance policy can be managed by the corresponding governance teams;
- **Data risk management:** Key functions of a data risk manager include detecting irregularities or defects in data series, and

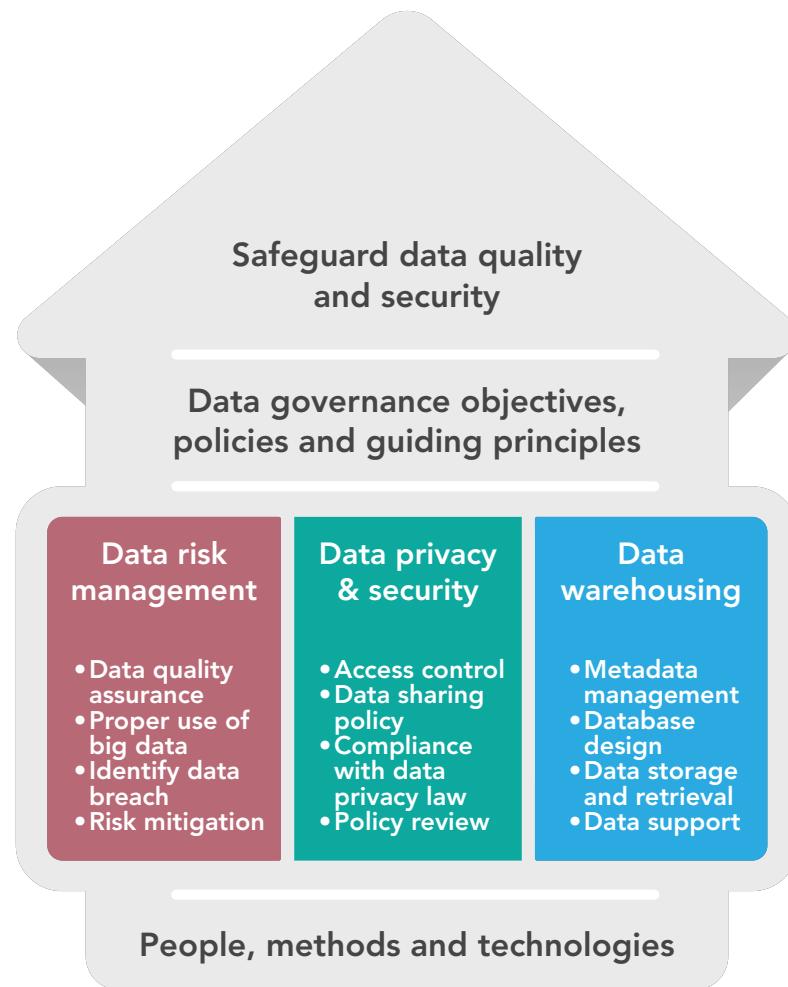
liaising with data vendors to assure and improve data quality. With the increasing use of big data in AI models, a data risk manager also needs to monitor the proper use of third-party information from the media and the internet, and take remedial actions if a data breach or misuse is identified;

- **Data privacy and security:** It is necessary to set separate layers of access control based on confidentiality and materiality across different data categories such as customer, corporate and analytical data to enhance data security. Data security officers need to ensure that the collection and use of customer data comply with regulations, and that data sharing with third parties, such as a credit reference agency, is in line with company policy; and
- **Data warehousing:** This involves the design of a proper centralised database to store and retrieve data efficiently and the maintenance of a comprehensive record of metadata such as data definition, source and usage. As such, the team needs to work closely with IT to build a company-wide infrastructure, and provide data support to the different business units.

<sup>9</sup> For a thorough discussion on data governance framework, please refer to *The SAS Data Governance Framework: A Blueprint for Success*, the SAS Institute, 2018.

Chart 2.3 summarises the key functions of a data governance framework including data risk management, data privacy and security, and data warehousing. Data governance policies are executed through these three units to safeguard data quality and security.

### Chart 2.3: Data Governance Framework: Structure And Functions



Source: HKIMR staff compilation.

It is important for the bank management to align the objectives of data governance to specific business goals, such as improving the efficiency of data management or meeting compliance requirements. During its implementation, management needs to choose a suitable strategy to communicate with major stakeholders, and find the right **people, methods** and **technologies** to execute the policy throughout the organisation.<sup>10</sup>

An effective data governance framework requires clear objectives from management, and a suitable strategy to execute the policy to safeguard data quality and security.

<sup>10</sup> Box 2.1 illustrates the issues encountered in launching a data governance framework that may yield different outcomes.

## 2.2.2: Challenges of implementing a data governance framework

The effective execution of data governance policies is not a straightforward process and requires the joint efforts of the IT team and relevant business units. In the initial stage, the management may take a sequenced approach by first building the core data governance functions, then adding new components guided by business needs and compliance requirements. This helps gain the support of staff once the importance of the safe and proper use of data has been communicated. Some common mistakes in the implementation of data governance policies may include:<sup>11</sup>

- (i) The absence of clear objectives and sound methods to execute the policy;
- (ii) Overlooking the company's corporate culture;
- (iii) Introducing drastic changes to existing policies on data use and protection; and
- (iv) Lack of a clear linkage between data governance objectives and business values.

A common problem often occurs after the launch of the data governance programme when data users view the programme as simply an IT issue and become passive or reactive in working with data governance teams. Fragmented data infrastructure, such as a lack of documentation of data ownership, could make it difficult to verify data quality and assign access rights. The shortage of resources and talent is also a common challenge faced by management in launching data governance programmes.

To overcome these challenges, data governance policy and decision-making should be transparent and clearly communicated. The management should remain flexible and pragmatic in designing and implementing a data governance framework that fits business needs and corporate culture. Data governance teams need to seek support and advice from IT and business units when building the infrastructure. It is also important to manage the expectations of major stakeholders. Data governance is an on-going process requiring periodic reviews of policies and practices.

The management should remain flexible and pragmatic in launching a data governance framework to gain support from staff.

<sup>11</sup> 10 Mistakes to Avoid When Launching Your Data Governance Program, SAS Institute, 2017.

### Box 2.1: Launching data governance programmes is not a straightforward process

In a white paper on data governance framework published by the SAS Institute, case studies on a regional bank and a global bank are used to highlight the importance of linking data governance policies to business goals.<sup>12</sup> In the case of the regional bank, management launched an initial data governance programme with broad support from different business units. After reviewing all types of data categories, it was found that the most problematic data issues were related to the phone numbers and seasonal addresses of customers, which had little strategic value to the bank. Consequently, management turned its attention to data problems with closer ties to business strategies.

In the global bank's case, planning had begun on the launch of a data governance framework to address increasingly complex compliance requirements and risk data aggregation principles. With these mandates, the data steward team identified the key data owners, consolidated the efforts of data quality assurance, and built a programme to demonstrate how company data could be managed to meet regulatory standards. The framework earned increasing support from management because it demonstrated its value to the bank.

These examples suggest that more traction is gained if the data governance initiatives can be tied to specific goals or business challenges facing the banks.

## 2.3: MACHINE LEARNING AND MODEL-RISK MANAGEMENT

The number of models used by banks incorporating big data analytics and ML techniques has been growing. Estimates by McKinsey show the number of models used by large institutions grew by 10–25% a year,<sup>13</sup> as banks and other financial institutions broaden the use of data-driven models in decision-making, such as credit scoring and fraud detection. However, these model-driven activities also expose banks to risks of misuse or over-reliance on quantitative models that may lead to significant losses if not properly managed.

Algorithms and statistical techniques used in models powered by ML are becoming increasingly sophisticated. Consequently, AI model risk has become a key area to be monitored by banks, especially for those with extensive use of AI applications. According to the Capital Requirements Directive (CRD IV) in Europe, AI model risk refers to potential losses incurred by banks as the decisions principally made by AI models could be subject to errors in the design, implementation or use of such models (Chart 2.4). Four factors that may lead to the improper use of AI models include:<sup>14</sup>

- **Human bias:** the psychological biases of AI model developers and users can affect outputs and result in unintended consequences. AI models may also make biased decisions reflecting social inequalities, even when sensitive data such as race and gender are excluded<sup>15</sup>;

<sup>12</sup> The SAS Data Governance Framework: A Blueprint for Success, the SAS Institute, 2018.

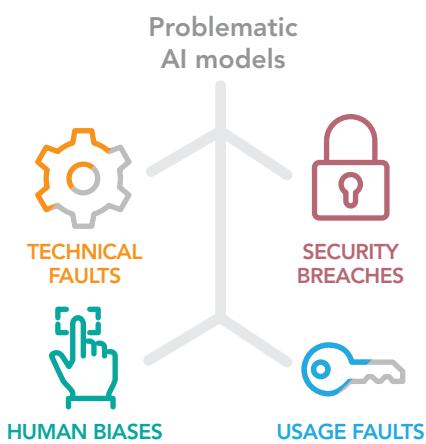
<sup>13</sup> See The Evolution of Model Risk Management, McKinsey, 2017.

<sup>14</sup> Deloitte (2019), The Evolution of Model and Algorithmic Risk: A Robust Model Risk Management Framework for Financial Institutions.

<sup>15</sup> <https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai>

- **Technical faults:** the absence of technical rigour in model design, training, testing and validation can lead to inaccurate or inconsistent outputs. This raises concerns given the insufficient quality of data and the scarcity of AI talent, which are common problems for banks in advancing AI applications<sup>16</sup>;
- **Usage faults:** the increased use of cloud computing and open source software has resulted in the democratisation and decentralisation of the development of AI models. Without proper validation by internal risk control units or seasoned model developers, flaws originated by using third-party models can result in false outputs and predictions to end users; and
- **Security faults:** security breaches can allow internal or external “actors” to manipulate the output of AI models. Studies have shown that it is relatively easy to engineer the output of AI models, even for leading pattern-recognition technologies that prove to be highly successful in classifying images, speech and data on consumer preferences.<sup>17</sup> AI models not robust to input manipulation could lead to wrong decisions.

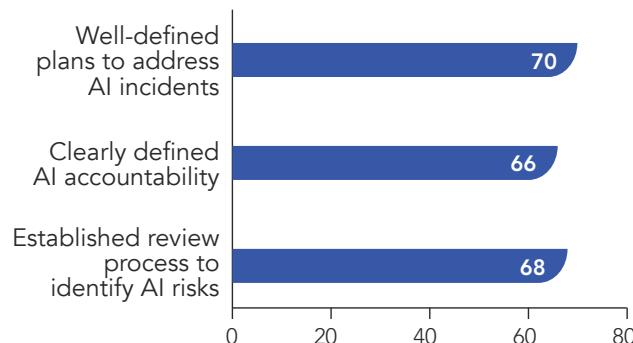
#### Chart 2.4: Risk factors that may lead to problematic AI models



Sources: Deloitte and HKIMR staff compilation.

In Hong Kong, banks are aware of the challenges from developing and implementing AI applications. The results of the HKMA AI Survey show that about two-thirds of banks utilising AI have well-defined procedures to address AI model defect cases, clear internal accountability and established review process to identify potential AI risks (Chart 2.5).

**Chart 2.5: Preparedness of banks in managing AI model risk**  
AI utilising banks (% share)



Note: AI-utilising banks refer to banks currently using or planning to use AI applications.

Sources: HKIMR staff calculations based on the HKMA AI Survey.

In Hong Kong, banks are aware of the risks of using AI models with about two-thirds of the survey respondents having well-defined processes to assess AI risks and address AI model defect cases.

<sup>16</sup> <https://www.forbes.com/sites/bernardmarr/2018/06/25/the-ai-skills-crisis-and-how-to-close-the-gap/#4e4c120e31f3>

<sup>17</sup> <https://www.nature.com/articles/d41586-019-03013-5>

### 2.3.1: Broader use of AI may increase banks' exposure to model risks

While AI models using big data and ML techniques have the potential to make more accurate data-driven decisions than traditional statistical models, they are still subject to the availability of relevant data. One example is the credit scoring models for making lending decisions to small and medium sized enterprises (SMEs) or individuals based on predicted probability of default. There are instances where the model outcomes may not be satisfactory with many false positives. In many cases, the model deficiency may be attributed to a lack of quality data such as credit history and the outstanding debt of borrowers, which are key factors in predicting default probability. This explains why the sharing of credit and loan data among banks through a centralised credit reference agency is important in improving lending decisions.

Another recent example, involving the use of the Apple Card (a credit card created by Apple Inc. and issued by investment bank Goldman Sachs) illustrates the reputational risk created by a possible bias in the model design. The Apple Card has been used by a wide range of customers in the US. Similar to credit scoring models adopted by banks, Apple uses its own algorithms to assign credit limits to its customers. In November 2019, the Apple Card was accused of sexual discrimination, based on a case where a much higher credit limit granted to the husband than his better-qualified wife, with a difference of 20 times the spending limit. This example raised concerns over the possible gender bias embedded in the model design. The incident prompted a regulatory scrutiny and investigation into the fairness of making credit limit decisions by the Apple Card company.

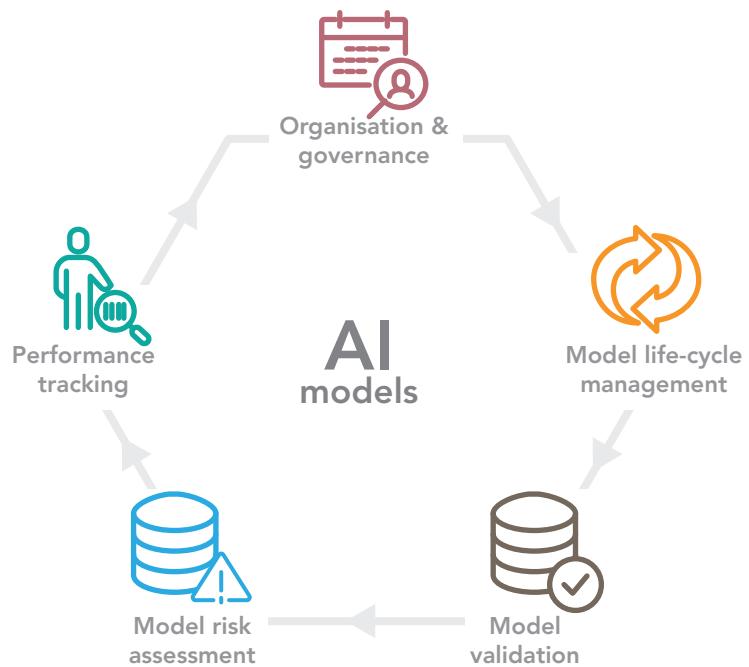
The above examples show the constraints faced by banks in developing AI models, and the unintended biases that could be built into the models based on social and cultural characteristics. They also highlight the importance of a rigorous validation procedure to assess the reliability of model outcomes and assure the quality of decisions made by AI models. Given that there is a wide spectrum of AI applications used by banks, it is desirable for the management to prioritise resources in managing AI model risks based on the materiality of model outcomes. For example, the impact of using chatbots to handle customer enquiries may be different than the one due to credit scoring used to making lending decisions. In the latter case, human intervention may be needed when inconsistent outcomes are identified.

### 2.3.2: Key elements in an AI model-risk management framework

In the aftermath of the Global Financial Crisis in 2008, regulators tightened oversight of the use of quantitative models by banks, including algorithmic trading and credit scoring. In response, banks strengthened internal controls on the quantitative models they used. With

the growing use of big data analytics and ML techniques, bank management needs to use a more robust approach to monitor and manage the risks of using AI models including: (i) organisation and governance; (ii) model life cycle management; (iii) model validation; (iv) model risk assessment; and (v) performance tracking (Chart 2.6).<sup>18</sup>

**Chart 2.6: Key elements of a model-risk management framework addressing AI risks**

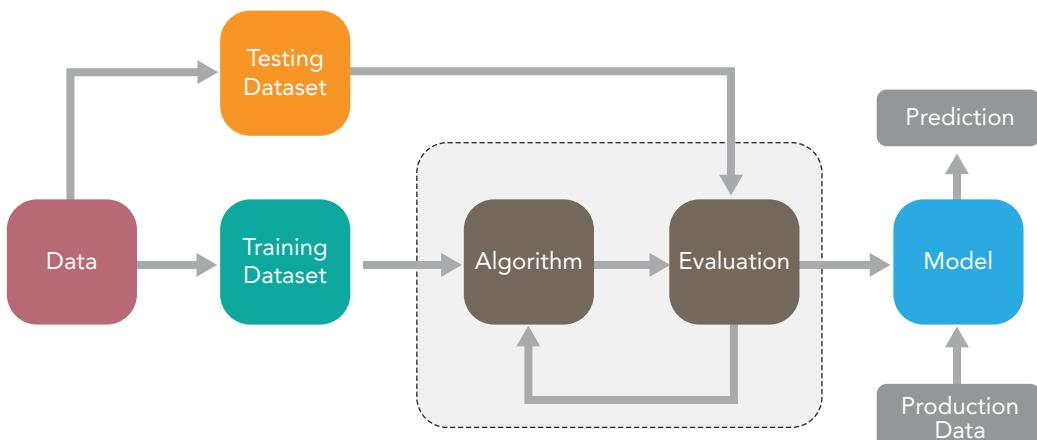


Source: HKIMR staff compilation.

<sup>18</sup> Deloitte (2019), *The Evolution of Model and Algorithmic Risk: A Robust Model Risk Management Framework for Financial Institutions*.

- **Organisation and governance:** The complexity of AI models suggests there may be a need for the management to establish an AI model risk control unit to oversee the design and use of AI models, and to carry out model validation. The unit should be an integral part of the risk management office, and explain the results of model risk assessment to management, internal auditors and regulators.
- **Model life cycle management:** The building of an AI model may involve different phases. The developer may start from using a small, pilot model where diverse data (or training dataset) are used to train the ML algorithm embedded in the AI model. The developer then has to evaluate the model outcomes and fine-tune the model design until consistent outcomes are obtained (Chart 2.7). During this process, the role of the model risk manager is to document different stages of development of AI applications, which will be stored in a centralised model inventory to facilitate model validation or remedial actions if needed.

**Chart 2.7: An illustrative life cycle of an AI model**



Source: HKIMR staff compilation.

- **Model validation:** One major function performed by the model risk manager is to verify the robustness of AI models by using a wide range of data and validation methods, such as back-testing and cross validation.<sup>19</sup> In this situation, the risk manager serves as a second line of defence by verifying the reliability of model outcomes. The manager also needs to ensure AI models are built in compliance with the bank's internal governance policy and regulatory requirements.
- **Model risk assessment:** This involves ranking the risk of AI models based on a basket of factors such as materiality, complexity of methodology, financial impact and performance soundness. Scores may be assigned based on the risk level of these attributes and aggregated to obtain an overall risk score or ranking for AI models. This measures the extent of the potential risk to the bank from using the AI model, and may be referenced to rationalise the resources allocated to tracking the performance of AI models with high risk and large impact on the bank. When there is a big jump in the risk score of an AI model, the manager needs to discuss this with the model's owner and report to the Chief Risk Officer.
- **Performance tracking:** This serves a number of purposes and is an essential step in identifying irregularities in model outcomes which form the basis for risk managers to require the owner of the model to take remedial action. Performance history is a useful reference for model owners to recalibrate and enhance AI models when new data or ML methods become available. In addition, the performance record is a component for the risk manager to evaluate the overall risk score of an AI model. Management can also refer to the performance history when reviewing the governance policy related to the use of AI models.

With the growing use of big data analytics and increased complexity of ML techniques, banks need to strengthen their model-risk management practices to safeguard the prudent use of AI models.

<sup>19</sup> Back-testing involves feeding historical data into an AI model and testing the accuracy of its outcome. Cross validation is to generate a new dataset using resampling method to evaluate the consistency of model outcome.

### 2.3.3: Challenges faced by banks in AI model-risk management

The complexity of AI models powered by ML techniques presents a number of challenges to banks. Based on the discussions with industry practitioners by data specialists and consultancy firms, there are several constraints faced by banks in managing risks associated with AI models.<sup>20</sup> First, the shortage of talent with AI and ML expertise makes it difficult for the risk manager to thoroughly perform risk

assessment and model validation. Second, insufficient data infrastructure, such as a reliable database and powerful computing capacity, undermines the efficiency with which models are validated and their performance tracked. Third, compliance with evolving regulatory requirements is another challenge facing banks that use AI models extensively. As regulators issue new guidelines and standards for the prudent use of AI technologies, compliance costs are likely to increase, particularly for these banks. (Table 2.1).

**Table 2.1: Challenges faced by banks in managing AI model risks**

<div style="text-align: center; border-radius: 50%; width: 50px; height: 50px; background-color: #1a237e; color: white; font-size: 24px; line-height: 50px; margin-bottom: 10px;">1</div> <p><b>SHORTAGE OF TALENTS WITH AI AND ML EXPERTISE</b></p> <ul style="list-style-type: none"> <li>• Stiff competition for data scientists with AI knowledge</li> <li>• Lack of expertise in assessing AI model risks</li> </ul>	<div style="text-align: center; border-radius: 50%; width: 50px; height: 50px; background-color: #a94a53; color: white; font-size: 24px; line-height: 50px; margin-bottom: 10px;">2</div> <p><b>INSUFFICIENT DATA INFRASTRUCTURE</b></p> <ul style="list-style-type: none"> <li>• Lack of quality data for model validation</li> <li>• Inadequate computing resources for tracking model performance</li> </ul>	<div style="text-align: center; border-radius: 50%; width: 50px; height: 50px; background-color: #ff9933; color: white; font-size: 24px; line-height: 50px; margin-bottom: 10px;">3</div> <p><b>COMPLIANCE WITH REGULATIONS</b></p> <ul style="list-style-type: none"> <li>• Challenges from evolving regulatory requirements</li> <li>• Increased costs of compliance</li> </ul>
---	---	---

Source: HKIMR staff compilation.

<sup>20</sup> Some of the constraints faced by banks in using ML-driven models can be found in *5 Machine Learning Mistakes — and How to Avoid Them*, SAS Institute, 2016.

To overcome talent scarcity, banks need to provide training to their staff on AI risk management. Employees with strong IT and mathematics backgrounds can be potential candidates for performing the tasks of monitoring and assessing AI model risks. Banks may also co-operate with universities and consultancy firms to offer training on data science and machine learning techniques to staff responsible for model-risk management.<sup>21</sup>

On improving data infrastructure, banks can establish data governance frameworks to enhance data quality and accessibility to various databases, and devote resources to upgrade the computational capacity of the model-risk management team. To cope with evolving compliance requirements, maintaining good communications with regulators is a major step for understanding existing regulations and adjusting corporate governance policy to comply with the required standards.

In broadening the use of AI models, banks need to overcome the challenges from talent scarcity, lack of reliable data and the evolving compliance environment.

## 2.4: CYBERSECURITY OF AI SYSTEMS

Cybersecurity is now becoming one of the key concerns of bank management, with the growing popularity of online and mobile banking. These developments are facilitated by greater IT efficiency driven by cloud computing.<sup>22</sup> Advances in technology have also increased the sophistication of cyberattacks using AI techniques. For example, malicious software can be used to engineer an attack that mimics the special features of bank customers, such as facial or voice patterns, to gain access to their accounts through online platforms.

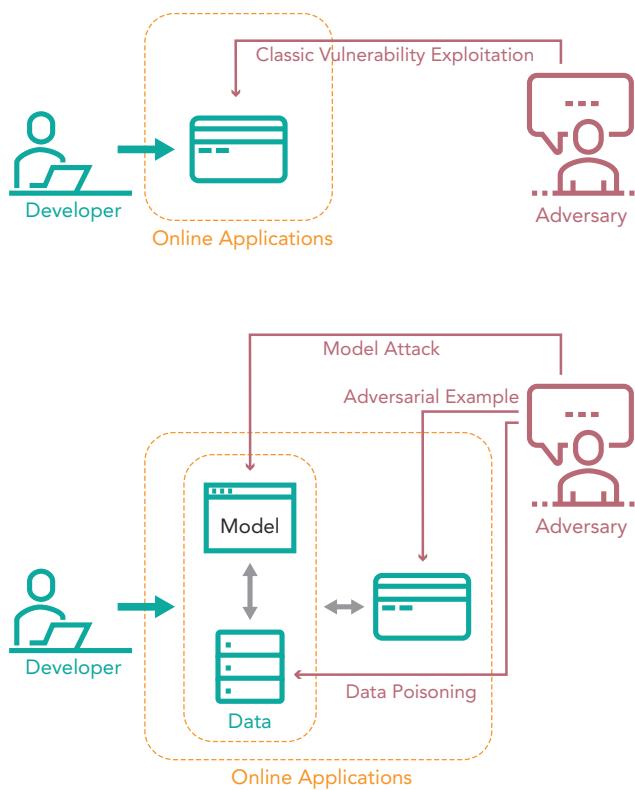
With the increasing use of AI applications in internet banking, malicious actors may use sophisticated methods to attack the core components of AI models. In the classic case of cyberattack, an adversary uses intrusive malware to attack the most vulnerable segments of online applications. The growing use of AI technologies in internet banking has opened a new array of cyber threats targeting the core components of AI systems. For example, the adversary can use data poisoning techniques where false data is introduced into the training dataset of AI models, resulting in inaccurate or inconsistent outcomes. Other techniques include crafting of adversarial examples to fool AI models or exploiting inherent weaknesses of the algorithm used in the applications (Chart 2.8)<sup>23</sup>. These new cyberattack techniques can put banks' AI systems at risk and undermine public confidence in the security of internet banking if the attacks result in serious disruptions to services or mass leakage of sensitive data.

<sup>21</sup> For recommendations on advancing AI development by banks in Hong Kong, please read *Reshaping Banking with Artificial Intelligence*, Chapter 6, published by HKMA in December 2019.

<sup>22</sup> Cloud computing improves efficiency of a company's IT resources through sharing data storage space and software applications on the cloud platform.

<sup>23</sup> European Commission (2020), *Robustness and Explainability of Artificial Intelligence*.  
[https://publications.jrc.ec.europa.eu/repository/bitstream/JRC119336/dpad\\_report.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC119336/dpad_report.pdf)

### Chart 2.8: Paradigm shift in cybersecurity of IT systems with AI components



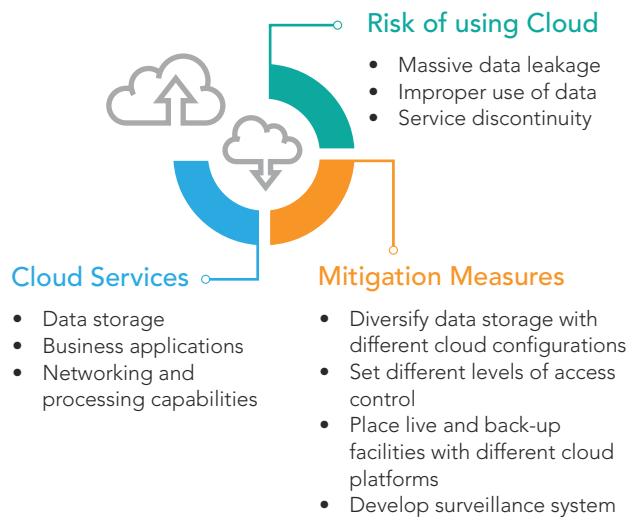
Sources: HKIMR staff compilation and European Commission (2020).

Banks need to strengthen their cyber defence systems as advances in technology have increased the sophistication of cyberattacks targeting AI applications.

### 2.4.1: Cloud computing as a new source of cyber threat

Apart from new techniques in cyberattacks using AI tools, another emerging source of cyber threat comes from cloud computing, which has become an essential part of the banking infrastructure for a growing proportion of transactions and payments handled by mobile or online banking. Cloud platforms offer on-demand network access to a shared pool of configurable computing resources, and is attracting intensive use by banks as an increasing number of AI applications are run on the cloud platform (Chart 2.9).<sup>24</sup>

### Chart 2.9: Cloud computing: functions, risks and mitigation measures



Source: HKIMR staff compilation.

<sup>24</sup> OFCO, HKSAR Government, 2018. [https://www.ogcio.gov.hk/en/our\\_work/information\\_cyber\\_security/government/doc/ISPG-SM04.pdf](https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM04.pdf)

While cloud computing has reduced the cost of IT solutions and become a major driver of business innovation, it also raises cybersecurity issues such as data security and the safe use of business applications including AI models. To mitigate the risk of massive data leakage, banks may diversify data storage with different cloud configurations.<sup>25</sup> For the most sensitive categories such as customer data, banks may store the information in a private cloud developed in-house by the IT department. The less sensitive categories, for example analytic data, can be saved with hybrid or public cloud servers.<sup>26</sup> Banks can also set different levels of access control to reduce the risk of leakage and improper use of data. In addition, they can place live and back-up versions of business applications and analytical tools with different cloud service providers. A surveillance system is another area that can be used to detect abnormal network activities and potential cyberattacks to cloud servers.<sup>27</sup>

Banks may diversify data storage with different cloud configurations such as public, private or hybrid cloud, to reduce concentration risk in cloud computing.

#### 2.4.2: Cybersecurity is critical to safeguarding data security and AI system

Given that AI tools are becoming more accessible, the probability of AI-based cyberattacks is also likely to increase. Banks need to allocate more resources to tackle this relatively new but significant threat, and should increase their IT budgets to enhance analytical tools to detect potential risks to their AI systems and online platform.<sup>28</sup>

<sup>25</sup> Many supervisory agencies provide guidelines on the selection and contracting processes with third parties, and on the continuous monitoring of their performance. The wider adoption of cloud outsourcing to a small number of providers creates concentration risk which could become systemic (Bank of England (2019b)).

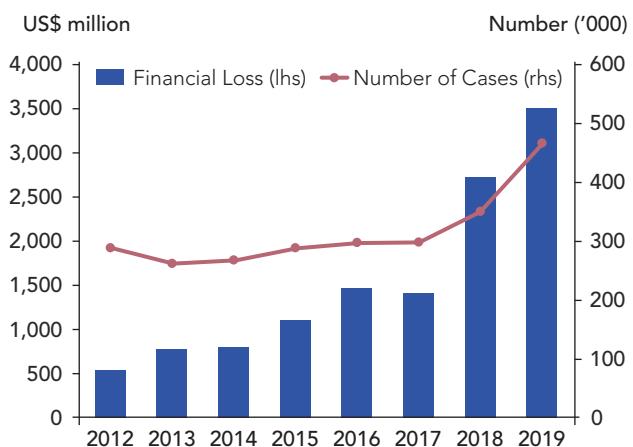
<sup>26</sup> A hybrid cloud is a mixture of private and public clouds.

<sup>27</sup> OFCO, HKSAR Government, 2018  
[https://www.ogcio.gov.hk/en/our\\_work/information\\_cyber\\_security/government/doc/ISPG-SM04.pdf](https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM04.pdf)

<sup>28</sup> A survey conducted by the SANS Institute shows that financial institutions on average use 10–12% of their IT budgets on system security.

Increasing incidence of cyberattacks have caused significant financial or data losses around the globe. According to statistics from the Federal Bureau of Investigation (FBI), the number of cyberattacks reported in the US and overseas locations increased by 60% between 2012 and 2019, with associated financial losses rising by more than five times to US\$3.5 billion in 2019 (Chart 2.10). It is anticipated that the broader use of AI applications will increase the risk of internet technology crimes, making AI-driven online banking more susceptible to new forms of cyber threats.

**Chart 2.10: Cyberattacks reported to FBI: number of cases and financial losses**



Source: FBI Internet Crime Reports.

#### 2.4.3: The evolution of cyber defence strategies adopted by banks

Traditionally, banks adopted a piecemeal approach to managing cybersecurity risks.<sup>30</sup> Under this operating mode, whenever a new type of cyber threat was identified, a new defence tool was deployed to address the risk. This resulted in a fragmented cyber defence system.

Over the years, banks have started adopting a structured approach to building a more robust system. This approach uses behavioural analytics and predictive tools to establish a security platform to detect abnormal activities throughout a company's IT network. Instead of detecting the occurrence of a breach, the enhanced security platform can identify the specific segments that are being affected by the attack, and the associated damages.

A structured approach offers a more comprehensive solution to cybersecurity, and better protection for banks' IT and AI systems. The key elements of a structured cyber defence system include the following five steps, which are summarised in Table 2.2:

- (i) Raising employee **awareness** of potential cyber risks, and creating a culture of shared responsibility for cybersecurity;
- (ii) Enhancing **protection** by using robust cyber defence tools such as multifactor or biometric authentication and conducting simulated attacks to assess the resilience of the cyber defence system;
- (iii) **Detecting** potential cyber threats using enhanced analytical tools such as behavioural analysis, predictive modelling and machine-learning techniques;
- (iv) Taking remedial **action** to minimise the damage caused by cyberattack, including maintaining internal and external communications on the event, implementing the contingency plan and investigating the attack; and
- (v) Implementing a **recovery** plan to restore public confidence and rebuild reputation, conducting a postmortem examination on the cause and impact of the attack and reviewing policies in strengthening cyber safety measures.

<sup>30</sup> A cybersecurity framework: Six steps to empowering your analytics by Mark Dobeck, Cleveland State University's College of Business.

**Table 2.2: A structured approach to cybersecurity: key elements**

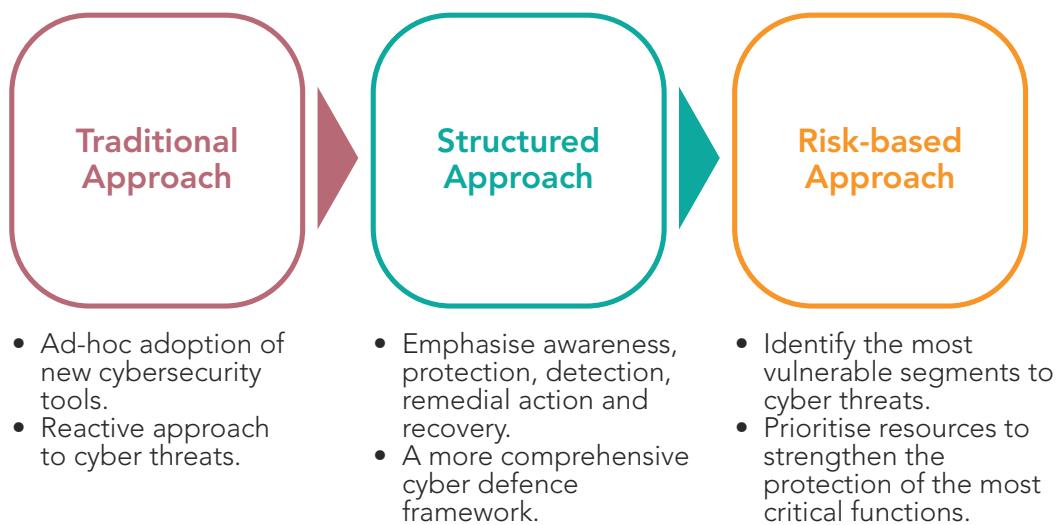
<b>Awareness</b> 	<ul style="list-style-type: none"> <li>• Raising employee awareness of cyber risks</li> <li>• Creating a culture of shared responsibility for cybersecurity</li> </ul>
<b>Protection</b> 	<ul style="list-style-type: none"> <li>• Using robust defence tools to deter potential cyber threats</li> <li>• Conducting simulated attacks to assess the resilience of cyber defence systems</li> </ul>
<b>Detection</b> 	<ul style="list-style-type: none"> <li>• Using enhanced risk detection methods (e.g., behavioural analysis, predictive modelling and ML techniques)</li> </ul>
<b>Action</b> 	<ul style="list-style-type: none"> <li>• Taking remedial action to minimise damage</li> <li>• Maintaining internal and external communications on the event</li> <li>• Investigation of the attack</li> </ul>
<b>Recovery</b> 	<ul style="list-style-type: none"> <li>• Implementing recovery plan to restore public confidence</li> <li>• Conducting postmortem examination on the attack</li> <li>• Reviewing cybersecurity policies</li> </ul>

Source: *A cybersecurity framework: Six steps to empowering your analytics* by Mark Dobeck, Cleveland State University's College of Business.

One limitation of the structured approach is that it tries to build control and monitor points across a wide spectrum of network activities without specific focus. However, cyber threats have evolved into different forms using new technologies, with more sophisticated techniques and specific targets. Applying a similar level of defence tools across all business areas subject to cyber risk would encourage inefficient spending and discourage cyber risk managers from devoting sufficient attention to areas with the highest vulnerability. A further step to improve efficient use of resources is to migrate to a risk-based approach, which emphasises strengthening the protection of most vulnerable segments to cyber threats. Chart 2.11 summarises the key features of cyber defence strategy at different stages.

With increasing cyber threats, banks are moving from the traditional piecemeal approach to a structured or risk-based approach to strengthen cyber defence systems.

**Chart 2.11: Different stages of cyber defence strategy**



Source: HKIMR staff compilation.

The migration from the structured to risk-based approach will not only reduce costs, but also strengthen the protection of the most vulnerable areas to cyberattacks. When implementing the risk-based approach, cyber risk managers need to identify and prioritise cyber risk measures, and focus on building appropriate controls on the most critical areas. This may involve the following steps:<sup>31</sup>

1. **Identifying and prioritising risks:** The risk manager gives precedence to different business functions and processes according to their contribution to company values, and then identifies and assesses their respective risks;
2. **Addressing risks:** The risk manager seeks to understand risk management tools and match them to identified risks, employing extra tools if necessary. Emphasis should be given to the cohesion of different control tools within the common risk management framework; and
3. **Monitoring risk-reduction performance:** While banks tend to stop the cyber risk review process after its implementation, it is important to create respective key risk and performance indicators to help monitor the effectiveness of different tools on cyber risk management.

#### 2.4.4: Challenges of implementing a robust cybersecurity framework

The highly digitalised nature of banking services and the increasing use of AI models underscore the importance of cybersecurity, which has become an indispensable part of safe banking. It is time for banks to invest more resources and manpower into identifying vulnerable segments to new cyber threats, and implementing remedial measures to enhance overall system security.

In Hong Kong, banks conducting simulated attacks to identify the weakest link in their cybersecurity systems, expressed concerns over the availability of qualified professionals to carry out the assessment.<sup>32</sup> To enhance the resilience of the banking sector to cyber threats and encourage talent development, the HKMA launched the **Cybersecurity Fortification Initiative** (CFI) in 2016 to strengthen banks' cyber defence systems, offering training to practitioners, and promoting intelligence sharing. As part of the initiatives under the **Cybersecurity Resilience Assessment Framework** (C-RAF), banks are required to assess their own cyber risk profiles and benchmark the level of defence and resilience

<sup>31</sup> The discussion is largely based on the report *The risk-based approach to cybersecurity* by McKinsey, October 2019.

<sup>32</sup> Based on the feedback from the banks participating in the Cybersecurity Fortification Initiative launched by the HKMA.

required to protect their AI systems against cyberattacks. The C-RAF includes the following steps:

- **Inherent Risk Assessment** — Banks are required to classify their cybersecurity risk into “low”, “medium” or “high” categories based on the outcome of the assessment.
- **Maturity Assessment** — Banks are required to determine whether their actual levels of cyber resilience are commensurate with their inherent risk, and to formulate a plan to enhance the maturity level.
- **Intelligence-led Cyber Attack Simulation Testing (iCAST)** — Banks that are assessed to have medium or high inherent risk are expected to conduct iCAST, which simulates real-life cyberattacks from adversaries with the help of relevant cyber intelligence agents.

To enhance cybersecurity awareness and technical capabilities of the practitioners, the HKMA launched a **professional development programme** under the CFI. It is a training programme for cybersecurity professionals developed by the HKMA in collaboration with the Hong Kong Institute of Bankers and the Hong Kong Applied Science and Technology Research Institute.

The existence of information asymmetry in the latest techniques and developments in cyberattacks makes it difficult for banks to adopt pre-emptive measures to fend off potential threats. To encourage intelligence and knowledge sharing, under the CFI, the HKMA launched a **cyber intelligence-sharing platform** in collaboration with the Hong Kong Applied Science and Technology Research Institute and the Hong Kong Association of Banks.

The objectives of the HKMA’s Cybersecurity Fortification Initiative are to enhance the cyber-resilience of banks in Hong Kong, offer training to practitioners and promote intelligence sharing.

# CHAPTER 3

## OVERSIGHT OF ARTIFICIAL INTELLIGENCE IN BANKING — A COMPLEX TASK

35

### POLICY RESPONSES, STRATEGIES AND CHALLENGES

- 3.1: Oversight of AI adoption by banks: some policy considerations
- 3.2: General principles of supervising AI adoption by banks: an international perspective
- 3.3: HKMA's supervisory approach to AI adoption by banks
- 3.4: New challenges to bank regulators in the age of AI and digitalisation

Technology Neutrality

Soundness

Supervision

Fairness

# 3 OVERSIGHT OF ARTIFICIAL INTELLIGENCE IN BANKING — A COMPLEX TASK

## POLICY RESPONSES, STRATEGIES AND CHALLENGES

36

### HIGHLIGHTS:

- Financial regulators supervising the adoption of AI by banks seek to balance the objectives of maintaining financial stability, consumer protection and nurturing innovation.
- Bank regulators around the globe have generally adopted the strategy of setting out guiding principles with a view to promoting a sound, fair, ethical and transparent use of AI technologies.
- In line with this practice, the HKMA applies the twin principles of technology neutrality and risk-based supervision on AI adoption by banks. Three sets of supervisory guidelines govern the prudent use of data analytics and AI models, and strengthen the resilience of cybersecurity systems.
- Regulators across jurisdictions recognise that new thinking is important when monitoring and assessing micro and macro-systemic risks when embracing AI in banking.
- From a micro perspective, the greater use of machine learning to train algorithms on larger and more diverse data sets, presents new complexities for bank supervisors.
- From a systemic perspective, the increased interconnectedness between banks and Big Tech firms may increase risks from market concentration and contagion. Keen competition from these firms may also boost risk-taking behaviour by banks.

### 3.1: OVERSIGHT OF AI ADOPTION BY BANKS: SOME POLICY CONSIDERATIONS

Banks should keep abreast of new digital technologies. Technology innovations are encouraging new entrants into the financial services industry, increasing competition in markets where the incumbent banks traditionally operate. Technology innovations also allow opportunities for gains in efficiencies and new business opportunities for the banks. From a social perspective, integrating AI technologies into banking services, such as credit scoring, can help promote financial inclusion, with decisions on lending to individuals and SMEs based on structured data (e.g., credit profile)

and unstructured data (e.g., spending patterns of borrowers), rather than their ownership of collateral. Given these potential private and social benefits, a key policy consideration is not to smother innovation with new and stringent regulations.

This suggests that regulators need to progressively adjust compliance requirements to integrate AI risks into their existing supervisory framework. Hence, the focus is on framing high-level or general principles to guide banks as they adopt new AI applications.

Big data are far more granular and multidimensional than data that have traditionally driven banking decisions. The more intensive use of big data by ML-driven models, such as algorithmic trading and credit scoring, can create new risks that need to be managed. As ML techniques become more commonly used by banks, regulators are likely to formulate more comprehensive supervisory guidelines and requirements to ensure the prudent use of ML models.

### 3.2: GENERAL PRINCIPLES OF SUPERVISING AI ADOPTION BY BANKS: AN INTERNATIONAL PERSPECTIVE

One fundamental rule for supervision is “proportionality” where the degree of scrutiny is calibrated according to the size of the potential risk. Likewise, new regulatory prescriptions should be limited when the risks are small<sup>33</sup>. For example, risks are greater when AI is used for automating business decisions (e.g., granting loans) than when it is used for routine checks (e.g., computing basic statistics). Large or more complex applications can have material impact on banks. This suggests that a given risk may not be scrutinised with the same intensity in all banks, and the range of AI expertise required at each of the three lines of defence<sup>34</sup> in corporate governance will depend on the scope and complexity of AI adoption by banks.

Many aspects of AI applications are already covered by existing regulations. Regulators are aware that overly stringent rules may hinder financial innovation but at the same time would not want to dilute the responsibility of banks’ management for the technical specifications of their AI models.

Therefore, supervisory agencies are currently focused on framing high-level or general

principles for banks’ use of AI. In terms of supervision, regulators emphasise the importance of proper and effective governance frameworks. Rigorous model validation procedures are essential to managing the performance and risks of AI applications by banks. As AI adoption progresses, regulators will need to keep these supervisory guidelines under constant review.

Regulators around the globe are framing high-level principles in supervising the use of AI by banks, as they are aware that overly stringent rules may hinder progress in financial innovations.

In November 2018, the Monetary Authority of Singapore put forward four principles on the use of AI and data analytics with the mnemonic FEAT, for fairness, ethics, accountability and transparency (MAS (2018))<sup>35</sup>. These principles aim at providing guidance to financial institutions in developing and implementing AI applications, emphasising the importance of accurate and unbiased model outcomes, accountability of senior management in AI adoption, and adequate disclosure of AI-driven decisions to customers. In July 2019, the De Nederlandsche Bank (DNB) added two additional principles on top of the FEAT proposed by MAS. These six high-level principles have the mnemonic SAFEST, accompanied by seventeen notes of guidance on how to make these principles operational. These six principles encompass the following key elements (Table 3.1).

<sup>33</sup> Institute of International Finance (IIF) (2019) argues that regulatory initiatives should be commensurate with the materiality of each specific use.

<sup>34</sup> The three lines of defence are: (i) managers with operational responsibilities in the business area; (ii) central risk management function, and (iii) the external audit reporting to the Board.

<sup>35</sup> MAS worked closely with the Personal Data Protection Commission and the Infocomm Media Development Authority in supervising AI adoption by financial institutions.

**Table 3.1: DNB's SAFEST principles on the use of AI by banks**

<b>S</b>	<b>SOUNDNESS</b>	<ul style="list-style-type: none"> <li>AI applications should be accurate, predictable and operate within the rules</li> <li>Ensure AI used for different aspects of the same element are consistent</li> <li>Explicit mechanisms to trigger review when AI produces odd outcomes</li> </ul>
<b>A</b>	<b>ACCOUNTABILITY</b>	<ul style="list-style-type: none"> <li>The board needs to understand and be responsible for AI risks</li> <li>Reliance on third parties would not be an excuse</li> <li>Use interpretable algorithms to achieve sufficient explainability<sup>1</sup></li> </ul>
<b>F</b>	<b>FAIRNESS</b>	<ul style="list-style-type: none"> <li>Avoid sensitive inputs (e.g., gender and age) that may introduce unintentional bias and unfair discrimination</li> <li>Document how personal data predict risks and financial outcomes</li> </ul>
<b>E</b>	<b>ETHICS</b>	<ul style="list-style-type: none"> <li>Rules such as data privacy and non-discriminatory decisions can be considered — such rules differ across jurisdictions and they can be changed under social or political pressures<sup>2</sup></li> </ul>
<b>S</b>	<b>SKILLS</b>	<ul style="list-style-type: none"> <li>Given the shortage of AI talents who possess adequate knowledge in banking, computer science and statistics, non-technical bank staff should acquire necessary IT skills and learn how to react to AI weakness</li> </ul>
<b>T</b>	<b>TRANSPARENCY</b>	<ul style="list-style-type: none"> <li>Document weaknesses in AI adopted and the data sets used</li> <li>Develop tools and interfaces that facilitate the traceability, explainability and communication of applications using AI techniques</li> </ul>

1. Croxson, Karen, Philippe Bracke, and Carsten Jung (2019): "Explaining why the computer says "no"" FCA Insight, May.

2. Human inputs provide a "double-lock on unethical instructions — on the part of the instructor and the instructed". (Proudman (2019)). Please also see Falk, Magnus (2019), "Artificial intelligence in the boardroom" FCA Insight, August.

Sources: DNB (2019) and HKIMR staff compilation.

Since the Global Financial Crisis in 2008, regulators around the world have encouraged banks to take a critical attitude towards all their models. The Federal Reserve's *Guidance on Model Risk Management* (issued in April 2011) highlights the critical role of a rigorous model validation framework<sup>36</sup>. It proposes that an effective model validation framework includes three core elements: (i) an evaluation of the conceptual soundness of the model; (ii) ongoing monitoring through process verification and benchmarking; and (iii) outcome analysis such as back-testing. Such model validation should include an independent party not involved in the model's development, implementation or use (HKMA (2019))<sup>37</sup>. Effective senior management oversight supported by appropriate incentive and organisational structures is essential.

Several supervisory authorities have noted that model validation frameworks need to be updated in line with the greater scale and complexity of ML-driven applications. A joint Bank of England (BoE) and Financial Conduct Authority (FCA) survey noted that the standard metrics for the quantitative evaluation of a model should be supplemented with other criteria such as explainability, simplicity and reliability. "Explainability" in a model context means showing how input variables contribute to both the model's aggregate results and explain individual outcomes. The HKMA AI Survey summarised the barriers to AI adoption faced by retail banks in Hong Kong, and identified "results of AI applications being difficult to explain" as one of the most important impediments.<sup>38</sup> In addition, material and complex ML models require more frequent validation than simpler models (MAS (2018))<sup>39</sup>.

The continuous life cycle of ML-driven models where the algorithm changes as it learns from new data requires safeguards. The findings in the joint BoE and FCA survey show that safeguards were used in only about half of all cases, underlining the need to build in "human-in-the-loop" mechanisms when AI-enabled decisions produce odd results.

<sup>36</sup> The ECB's Guide to Internal Models (issued in November 2018) also underscores the importance of implementing a model risk management framework covering model governance, risk control on the use of models, model validation and internal audit.

<sup>37</sup> Hong Kong Monetary Authority/HKMA (2019): *High-level principles on artificial intelligence*, November.

<sup>38</sup> *Reshaping Banking with Artificial Intelligence*, page 88, HKMA, December 2019.

<sup>39</sup> Monetary Authority of Singapore/MAS (2018): *Principles to promote fairness, ethics, accountability and transparency in the use of artificial intelligence and data analytics in Singapore's financial sector*, November.

### 3.3: HKMA'S SUPERVISORY APPROACH TO AI ADOPTION BY BANKS

The stance of the HKMA on the use of technology by banks is based on two principles — technology-neutral and risk-based supervision.<sup>40</sup> Technology neutrality implies that the regulator will not introduce undue exemptions or requirements simply because certain types of novel technologies are used by banks. The aim is to provide a level-playing field and a conducive environment for banks to explore and develop new technologies to enhance operational efficiency.

The risk-based approach to supervision suggests that the regulator will focus on potential risks arising from the use of technologies when framing regulatory requirements. Hence, banks using more complex forms of AI applications with greater customer impact would be scrutinised more closely than banks using simpler versions of AI.<sup>41</sup> These two principles seek to foster the development of new AI applications in banking while safeguarding the prudent management of technology risks.

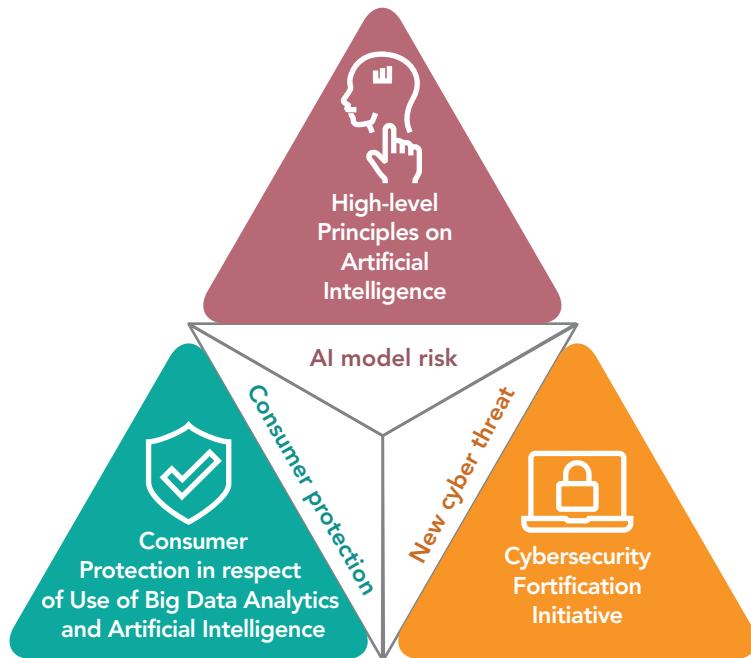
The HKMA applies the twin principles of technology-neutral and risk-based supervision for AI adoption by banks in Hong Kong.

The HKMA has developed several supervisory guidelines for banks to follow when applying AI in their business models. These guiding principles aim at setting out consistent regulatory standards for AI adoption by banks, and strengthening corporate governance in three key areas — consumer protection, AI model-risk management and the cybersecurity of AI models. Chart 3.1 shows how these guidelines fit into the supervisory framework of AI adoption by banks. The *High-level Principles on Artificial Intelligence* govern the design, implementation and validation of AI models. The principles on *Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence (BDAI)* by Authorised Institutions uphold consumer protection in the use of big data analytics and AI by banks. The *Cybersecurity Fortification Initiative* strengthens the resilience of banks' IT systems to malicious attacks.

<sup>40</sup> inSight article on *Risk-based and technology-neutral — the HKMA's supervisory approach to financial technology (Fintech)*, HKMA, March 2016.

<sup>41</sup> Differences in systemic risk are also relevant (Restoy (2019)).

**Chart 3.1: HKMA's supervisory guidelines related to AI adoption by banks**



Sources: HKMA and HKIMR staff compilation.

### 3.3.1: Guiding principles on the design and implementation of AI models

The HKMA's circular on the *High-level Principles on Artificial Intelligence* emphasises the importance of prudent risk management in the design, implementation and validation of AI models by banks. Three key aspects are identified — governance, application design and development, and ongoing monitoring and maintenance.<sup>42</sup>

- (1) **Governance** covers accountability and responsibility in adopting AI applications in performing banking functions. Bank management is accountable for the outcomes of AI applications, such as the decisions or recommendations made by AI models. Management needs to establish a robust governance framework to oversee the design and implementation of AI models, mitigate potential risks and take remedial actions if needed. The responsibilities of the three lines of defence (i.e., front-line office, risk control and internal audit) should be clearly defined to ensure prudent use of AI applications.

<sup>42</sup> Circular on *High-level Principles on Artificial Intelligence*, HKMA, 1 November 2019.

42

(2) **Design and development of AI applications** encompass seven main elements to cover three key stages of building an AI model, namely data input, model design and model output. Data input covers elements that assure data quality such as accuracy, completeness, timeliness and consistency of data used in AI models. It is desirable for the management to put in place a clear data governance framework to ensure data quality.

The proper design of an AI model should also meet certain standards. First, there should be sufficient expertise to design and implement AI models. Banks often work with external parties in developing new AI applications, but they need to conduct due diligence and periodic reviews of third-party vendors. Bank management and developers of AI models need to have an adequate understanding of how the models work, and be able to explain the design and operation of AI models to all relevant parties.

AI models should be validated and audited, while ensuring that AI-driven decisions are ethical, fair and transparent. Model validation is performed before implementation, to confirm the model's accuracy and appropriateness. Model

auditability includes tracking and documentation of the performance of AI models for monitoring and risk assessment purposes. Apart from accuracy and consistency in model output, AI-driven decisions should not be biased against any group of customers.

(3) **Monitoring and maintenance** cover four dimensions throughout the life cycle of AI models. These include ongoing monitoring and periodic reviews of model performance, complying with data privacy and protection requirements, implementing effective cybersecurity measures to fend off new forms of adversarial attacks, and putting in place risk mitigation measures and contingency plans for when AI models fail.

### 3.3.2: Consumer protection principles on the use of big data and AI by banks

This set of guiding principles focuses on consumer protection aspects in respect of the use of BDAI-driven models by banks.<sup>43</sup> The guidelines highlight the importance of upholding the principles of consumer protection when using BDAI applications. The objective is to protect consumers' interests, which in turn is expected to enhance customers' confidence in using banking services adopting BDAI. The principles cover four key areas in consumer protection for banks' use of BDAI applications, namely: (i) governance and accountability; (ii) fairness; (iii) transparency and disclosure; and (iv) data privacy and protection.

On **governance and accountability**, the emphasis is on the accountability of the board and senior management of banks for all the BDAI-driven decisions and processes, and an appropriate level of explainability and proper validation of BDAI models. According to the guidelines, appropriate governance, oversight and accountability framework should be established and documented. The use of BDAI models should be in line with the consumer protection principles set out in the *Code of Banking Practice and the Treat Customers Fairly Charter* issued by the HKMA. On **fairness**, the decision or outcome driven by BDAI models should be objective, consistent, ethical and fair

to customers. There should be possibility of manual intervention to mitigate irresponsible lending decisions where necessary. On **transparency and disclosure**, banks should disclose that the relevant service is powered by BDAI technology prior to providing banking services to customers, and explain on the types of data used and the factors affecting BDAI-driven decisions, upon customers' request and where appropriate.

With **data privacy and protection**, the collection of personal data by banks and their use in BDAI applications should comply with the *Personal Data (Privacy) Ordinance* (PDPO). Banks are also encouraged to observe and follow the good practices related to BDAI and Fintech recommended by the Privacy Commissioner for Personal Data. Where request for consent to the collection and use of personal data in relation to a banking product or service powered by BDAI technology is required, banks should ensure that such consent is as clear and understandable as possible in the interests of ensuring informed consent. To enhance data privacy protection, banks are expected to consider embedding data protection in the design of a product or system from the outset (i.e., "privacy by design")<sup>44</sup>, and collecting and storing only the minimum amount of data for the minimum amount of time (i.e., "data minimisation").

<sup>43</sup> Circular on Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions, HKMA, 5 November 2019.

<sup>44</sup> Apart from adhering to "privacy by design", a closer interface could be forged between regulated entities, Fintech service providers and enforcement authorities in building up an inclusive ecosystem.

### 3.3.3: Cybersecurity issues arising from the broader use of AI applications

One operational risk of great concern following the wider use of AI by banks is the emergence of new threats to cybersecurity. Phishers and fraudsters can use AI technologies to build powerful and adaptable tools to hack or attack specific segments of banks' computer systems.<sup>45</sup> The HKMA in its circular on *High-level Principles on Artificial Intelligence* has warned about these new cyber threats, such as data poisoning and adversarial attacks that exploit AI models through data manipulation. To safeguard the AI and IT systems against these risks, the HKMA requires banks to put in place effective security controls to counter such attacks, and to keep abreast of and remain vigilant to emerging security threats and the corresponding defence measures. The *Cybersecurity Fortification Initiative* (CFI) launched by the HKMA in 2016 has also strengthened banks' cyber defence systems to new forms of attack.<sup>46</sup>

The increasing cyber risks around the world stimulated by new technologies have become a significant concern for central banks and financial regulators. For example, a report by the Basel Committee has warned that data sharing in open banking platforms expands the surface area for cyberattacks.<sup>47</sup> A large and widespread cyberattack on the computer systems of banks could have systemic effects. International bodies and regulatory authorities are looking for a more consistent and coordinated regulatory landscape to strengthen the banking sector's cyber defence systems.

Three sets of supervisory principles governing the use of AI by banks include data analytics and consumer protection, AI model design and validation, and cybersecurity of AI applications.

## 3.4: NEW CHALLENGES TO BANK REGULATORS IN THE AGE OF AI AND DIGITALISATION

The complexity arising from the oversight of AI adoption can be analysed from both the micro and the macro perspectives. From a micro perspective, AI models powered by ML or other advanced algorithms are usually sophisticated and difficult to comprehend. Therefore, regulators need to better understand data science and programming when assessing whether the assumptions used and design of AI models are sensible, and whether the decisions made by AI models are reasonable, consistent and without bias.

<sup>45</sup> Brainard, L (2018): *What are we learning about Artificial Intelligence in financial services?* Speech at Fintech and the New Financial Landscape, Philadelphia, Pennsylvania. 13 November.

<sup>46</sup> The cybersecurity measures proposed under the CFI are discussed in Chapter 2 section 2.4.4.

<sup>47</sup> Basel Committee on Banking Supervision/BCBS (2019): *Report on open banking and application programming interfaces*, November.

From a macro-systemic perspective, the growing use of AI models in performing banking functions may increase the procyclicality of banks' behaviour and the interconnectedness between banks and Big Tech firms. Banking regulators also need to co-operate with the authorities overseeing data privacy and cybersecurity to strengthen the supervisory framework on AI adoption.

### 3.4.1: Challenges faced by regulators in supervising use of AI models: a micro perspective

Throughout the life cycle of AI models, data input, model design and validation could pose new risks to banks. To safeguard the proper use of AI applications, banks should strengthen their risk management systems to monitor and mitigate the risks of data breaches or misuses, and carry out rigorous validation procedures to assess the reliability of model outcomes. The role of regulators is to ensure that banks have adequate and effective internal controls and processes to manage risks associated with AI applications, and require bank management to take remedial action if loopholes are found in their governance frameworks.

The identification of the most vulnerable areas in banks' AI risk control frameworks could pose new challenges to regulators. One inherent risk of any data-driven model is that it may be vulnerable to manipulative or

collusive activities by fake or real customers. Detecting data deficiency is complex and requires specialised skills such as data science and statistics, and therefore banks need to have the right people and methods to uphold data quality and accuracy. Regulators need to strengthen oversight of data quality, which will assume greater importance in a digitalised banking environment.

The challenges in identifying possible defects in the design of AI models mainly come from two fronts, the complexity of **data analytics** and **ML algorithms** embedded in the model. Table 3.2 highlights some of the key challenges faced by regulators in supervising AI adoption by banks. In general, decisions driven by ML models could be less transparent and difficult to explain. For example, trading algorithms that include market mood or behaviour of market participants in AI models may increase market contagion<sup>48</sup> and procyclicality.<sup>49</sup>

From a micro risk perspective, the greater use of data analytics and ML algorithms in AI models present new complexities for bank supervisors.

<sup>48</sup> BaFin (2019) discusses how to counter the increased risk of the domino effect with increased AI adoption by financial institutions.

<sup>49</sup> It is also true that ML applications could reduce procyclicality. For instance, banks could use transaction data to finely tune credit decisions during downturns, by identifying credit-worthy customers more precisely and by reducing the procyclical dependence on collateral valuations.

**Table 3.2: Challenges faced by regulators in supervising AI adoption by banks**

- More advanced techniques in data analytics require new skills for regulators.
- Regulators need to maintain a clarity of communications with model developers to understand the logic behind the statistical outcomes.
- Banks should explain to regulators material decisions including discontinuing a model or changing a data set.

### Data Analytics

- Operation of ML-driven models is similar to a “black box”, with results emerging without simple explanations.
- Increased complexity for regulators to assess the underlying model risks.
- Decisions driven by ML-models could amplify contagion through interbank or business connections.

### ML Algorithm

Source: HKIMR staff compilation.

Given the complexity of verifying data quality and ML algorithms used in AI models, the **results of model validation** become an important metric for regulators to evaluate the accuracy and reliability of model outputs. There are several commonly used methods for regulators in assessing model validation results. One may compare model outcomes either against a benchmark or against what a non-ML model would have produced. Another method is data validation by using historical or out-of-sample data to test whether the outcomes generated from the model are consistent.

Regulators need to equip themselves with knowledge of AI and data analytics to cope with the increased complexity of AI models used by banks. For banks, a fundamental challenge in managing radical technological change is to ensure that the technical skills of staff are kept up-to-date with new developments in the design and implementation of AI applications. Regulators may need to develop some metrics to assess the competency of the bank’s AI staff such as education background, years of relevant experience and professional qualification. Risk managers and model users also need to understand how specific computer-based procedures could go wrong, and explain to regulators contingency plans and the triggers for human intervention.

Regulators need to equip themselves with knowledge in AI and data analytics to cope with the increased complexity of banks' AI models.

### 3.4.2: Challenges faced by regulators in managing systemic risks arising from AI adoption: a macro perspective

The supervisory framework for AI adoption requires oversight over a widening range of activities as the banking industry goes through a digital and technological transformation. This includes data collection and protection, new interconnections and the security of open banking operating on internet platforms. Digital technologies tend to make financial links between banks and non-banks more pervasive. Capital market-like intermediation may take new forms, revealing possible gaps notably in macro-prudential regulations.

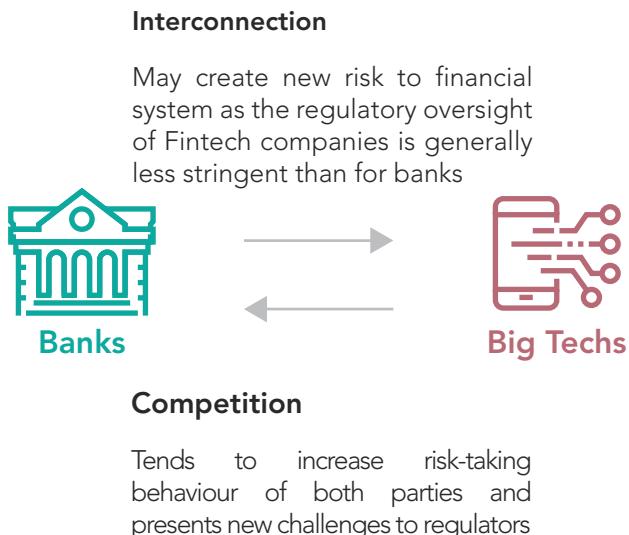
Effective supervision requires bank regulators to strengthen co-operation with public authorities responsible for non-financial firms heavily engaged in Fintech activities. Rules applying to such companies will be shaped by government policies on competition and

consumer protection (including data privacy) in addition to financial stability. One difficulty is that countries weigh these three considerations quite differently<sup>50</sup>. Another issue is that the initiative for any new regulations for Fintech companies may not necessarily rest with bank supervisors. There is a need for bank supervisors to establish a mechanism to exchange data and intelligence with other regulatory authorities to enhance the oversight of AI adoption by banks. One example of collaboration among regulators can be seen from the issuance of circular on *Use of Personal Data in Fintech Development* by the HKMA in May 2019. The circular encourages banks to adopt the good practices advocated by the Office of the Privacy Commissioner for Personal Data in collecting and using personal data for Fintech development.

From a macro perspective, **increased interconnectedness** and **competition** between banks and Big Tech firms may have systemic implications on the financial system. Growing interconnectedness between banks and Fintech companies, either in the form of affiliation or through various business channels, may create new risks to the financial system as the regulatory oversight of Fintech companies is generally less stringent than for banks. Another scenario posing systemic risk is increased competition between banks and Fintech companies. This will tend to increase the risk-taking behaviour of both parties and present new challenges to regulators (Chart 3.2).

<sup>50</sup> The graph on the regulatory compass for Big Techs in finance in BIS (2019) shows that rules adopted in different jurisdictions weigh these considerations very differently.

### Chart 3.2: Interconnection and competition between banks and tech firms

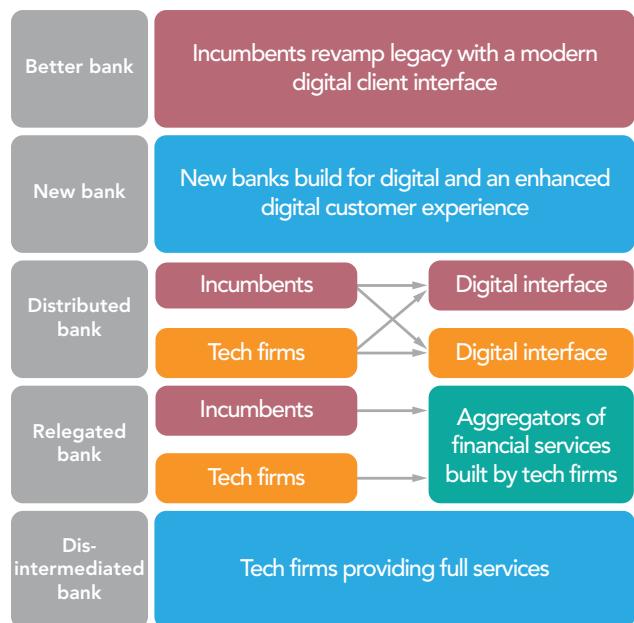


Source: HKIMR staff compilation.

From a macro-systemic perspective, increased interconnectedness and competition between banks and Big Tech firms may increase the risks of market concentration and contagion, as well as risk-taking behaviour.

The competitiveness of banks in a digital environment has attracted much debate. A consultative document issued by the Basel Committee on Banking Supervision (BCBS) outlined five scenarios on the possible transformation of banks in the age of technology.<sup>51</sup> At one end of the spectrum was the “better bank” scenario where incumbent banks readily adopt new technologies to retain customers and market share. At the other end was the “disintermediated bank” scenario where customers get their financial services from a myriad of Fintech companies, while banks ceased to play any important role in financial intermediation (Chart 3.3). Such a fragmentation in the financial value chain could create both regulatory gaps and overlaps.

### Chart 3.3: Five possible scenarios as banks undergo digital transformation



Note: These five scenarios are not mutually exclusive and the evolution of the banking industry may result in a combination of scenarios.

Sources: BCBS (2018) and HKIMR staff compilation.

<sup>51</sup> BCBS (2018): *Sound practices: Implications of fintech developments for banks and bank supervisors*, February.

The outcome of this competitive struggle will depend on many factors and is highly uncertain. One of the roles of regulators is to ensure that innovations in the provision of financial services do not put incumbent banks at a regulatory disadvantage. Policymakers may also need to think of a regulatory framework that takes into account the macroeconomic and financial stability benefits of a safe and sustainable system of financial intermediation handled by banks. As noted by the Financial Stability Board, one of the challenges faced by regulators in a digital age of banking is to consider how far "the resilience of incumbent financial institutions and the viability of their business models might be affected by their interlinkages with and competition from Big Tech firms."<sup>52</sup>

While many believe that banks can survive this wave of digital and technological transformation, the competitive threat from Fintech companies is a reality. At present, Fintech companies have developed their bank-like activities in partnership with incumbent banks. In future, however, they might increasingly deal with many banks and other specialised firms. This would entail a huge rise in the number of market connections, creating new and opaque systemic risks. Fintech companies that reach a certain scale in terms of assets might need to be brought within the regulatory perimeter of central banks and financial regulators.

Another potential systemic risk arising from the broader use of AI by banks is that it could aggravate the **too-big-to-fail problem**. The reasoning here is that the gain from economies of scale in the adoption of AI may increase concentration in the banking industry. A small number of bigger banks may dominate the market with monopolistic power, creating greater homogeneity in reaction to shocks. Such new forms of systemic risk may require new types of macro-prudential regulation.

The growing popularity of open banking could also pose systemic threats as it provides third-party financial service providers open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (APIs). The policy challenge is to meet such demands in ways that neither compromise the safety of the financial system nor rigidify particular mechanisms. The BCBS suggested that "banks and bank supervisors will have to pay greater attention to risks that come with the increasing sharing of data and growing connectivity between banks and various parties."<sup>53</sup>

These developments warrant ongoing monitoring of the impact of broader use of AI by banks and other financial institutions on financial stability.

<sup>52</sup> Financial Stability Board/FSB (2019): *Big tech in finance: market developments and potential financial stability implications*, December.

<sup>53</sup> BCBS (2019): *Report on open banking and application programming interfaces*, November.

# CHAPTER 4

## AI-AIDED COMPLIANCE AND SUPERVISION

HOW WILL REGTECH AND SUPTECH CHANGE THE LANDSCAPE OF COMPLIANCE AND BANKING SUPERVISION?

4.1: The potential of AI in Regtech and Suptech applications

4.2: Role of policymakers in fostering AI development in banking

Suptech  
Digital Reporting

Regtech

Machine  
Readable  
Regulation

# 4 AI-AIDED COMPLIANCE AND SUPERVISION

HOW WILL REGTECH AND SUPTECH CHANGE THE LANDSCAPE OF COMPLIANCE AND BANKING SUPERVISION?

## HIGHLIGHTS:

- Both banks and financial regulators are exploring the use of AI to automate the compliance procedure and assessing the benefits of integrating AI into the supervisory process to improve efficiency.
- Currently, most AI applications used in compliance, or Regtech, are mainly in regulatory reporting and fraud detection given availability of data and clearly defined requirements. In many cases, including investigation of suspected fraud cases or financial crimes, human intelligence is still required.
- The use of AI in supervision, or Suptech, is gaining traction. Regulators are using AI technologies to automate data collection from banks and exploring the feasibility of introducing machine-readable regulations. Advances in application programming interfaces will allow regulators to have direct access to banks' own reporting systems to gain additional insights from both structured and unstructured data.
- Policymakers can foster the proper use of AI by providing a favourable environment and a transparent supervisory framework. Policy initiatives to strengthen public-private co-operation could be useful, particularly in promoting knowledge exchange, experience sharing and talent development.

51

## 4.1: THE POTENTIAL OF AI IN REGTECH AND SUPTECH APPLICATIONS

Digitalisation and new AI technologies could streamline regulatory compliance (Regtech) and strengthen supervisory oversight (Suptech). For Regtech, supervisory agencies and banks are exploring using AI technologies to streamline reporting for compliance purpose. For Suptech, new technologies will allow supervisors to access and analyse the huge amount of structured and unstructured data (e.g., text or messages) maintained by banks in their own systems.

In principle, the development and alignment of new technologies used in Suptech and Regtech will be beneficial for both regulators and banks. Regulators will be accurately and quickly informed about the changing risk exposures of banks, and banks will find their reporting burden reduced.

In practice, however, this ambitious task will require careful preparation over some years. As pointed out by the BoE, the shortcomings of the current reporting system reflect not only inflexible reporting design but also the inherent constraints arising from the different business models of the banks (hence heterogeneity in their data) and the different objectives of the regulators (hence heterogeneity in their data requests)<sup>54</sup>. To improve the efficiency of data submission and regulatory reporting by banks, supervisory authorities are using AI technologies in automated reporting. One example is a pilot project undertaken by the BoE on digital regulatory reporting (DRR) in specific areas to improve clarity and shared understanding on the rules and data requirements through the establishment of a collaborative platform with banks.<sup>55</sup>

Advances in application programming interfaces (APIs) have made it more feasible for the regulator to “read” the bank’s own management information (MI) systems. Any inconsistencies between MI and the bank’s published accounts or regulatory reports can be identified. The rapid advancement in computer techniques in Natural Language Processing (NLP)<sup>56</sup> allows regulators to examine whether the Boards of different banks are concerned about the same risks. Reports on specific banks appearing in the international press can also be quickly collated and analysed.<sup>57</sup>

Advances in technology such as automation in regulatory reporting and APIs will improve efficiency and effectiveness in compliance by banks and risk monitoring by regulators.

#### 4.1.1: What Regtech can and cannot do

The scope of using Regtech by banks in meeting regulatory requirements is expanding. New technology has been used to automate the report-generating process by producing machine-readable banking returns for submission to regulatory authorities. Banks have also broadened the use of Regtech to identify misconduct behaviour and operational risks, as well as detect suspicious fraud cases and financial crimes.

Currently, Regtech is mostly applied in areas related to regulatory reporting. However, human intelligence regarding the scope of data reporting to regulators remains irreplaceable. Table 4.1 lists the tasks that can and cannot be performed by Regtech currently.

<sup>54</sup> See Bank of England (2020) report, which recognises that the regulator collects data from banks in a process that is “costly, takes time, is relatively inflexible, and involves a degree of duplication.”

<sup>55</sup> Following the van Steenis (2019) review, the UK’s Financial Conduct Authority conducted a pilot project for DRR on mortgage lending (FCA (2019). It found that part of the cost of the current approach to reporting comes from ambiguities in the regulations. In addition, it found that the automation of reporting by banks was often impeded by legacies of multiple computer systems.

<sup>56</sup> NLP is a branch of artificial intelligence that helps computers understand, interpret and manipulate human language. NLP draws from many disciplines, including computer science and computational linguistics to fill the gap between human communication and computer understanding.

<sup>57</sup> It is instructive to note that NLP techniques are not yet sufficiently developed to replace structured regulatory reports.

**Table 4.1: What Regtech can and cannot do**

<b>Can Do</b>		
		
Application of ML algorithms and AI technology can lower the rate of false alarms in performing AML and client due diligence functions.	Compliance reporting functions can be enhanced by (i) common reporting taxonomy; (ii) shared data repository; and (iii) the use of APIs by regulators to 'read' the data directly from banks' own systems.	Natural Language Processing offers new ways to monitor banks' sentiment and identify inconsistencies between banks' internal management information and published versions.
<b>Cannot Do</b>		
		
Human intelligence regarding the scope of data reporting to regulators is still irreplaceable.	Human investigation is still required for verifying detected suspicious fraud cases and financial crimes.	Human input is still necessary for internal oversight of the compliance framework, such as identifying potential compliance loopholes.

Source: HKIMR staff compilation.

#### 4.1.2: What are the prospects and limitations of using AI in Regtech?

Regtech integrated with AI and ML techniques can help perform tasks of greater complexity. For example, banks may use NLP to automate the regulatory review process. Aided by AI and Robotic Process Automation (RPA)<sup>58</sup>, banks could organise data conforming to reporting requirements, and submit real-time operational and transaction data to regulators. With advances in client digitalisation and identity authentication, the success rate in fraud detection has improved. AI technologies can also prioritise suspected fraud cases based on specific risk ratings to rationalise efforts of investigations. In some advanced use cases, AI is used to enhance consumer protection by matching the sales of investment products with customers' spending behaviour or their risk profiles.

While the application of advanced techniques in Regtech can improve compliance efficiency and reduce human error, it is not expected to replace human judgement as there could be the possibility of introducing unintended bias when using AI to identify compliance issues. Given the complexity of ML techniques used by banks, transparency and governance of the use of AI in meeting regulatory requirements will become more important when the use of Regtech by banks gains more traction.

The use of AI in compliance, or Regtech, improves regulatory reporting and fraud detection by banks, but human input is still needed for internal oversight of the compliance framework.

#### 4.1.3: What Suptech can and cannot do

Suptech can improve data collection from banks such as regulatory reporting and data management. Aided by data analytic tools, regulators can obtain additional insights from granular data for market surveillance and micro and macro-prudential supervision. Given these advantages, central banks are making greater use of Suptech. For example, the National Bank of Austria has developed a reporting platform linking to banks' IT systems for the seamless transmission of critical and confidential information. The UK's FCA is engaging in a proof-of-concept for the use of chatbots to interact with supervised entities, and studying the feasibility of machine-readable regulations focusing on the area of digital regulatory reporting. In Australia, the Securities and Investments Commission (ASIC) has launched a market surveillance system for real-time monitoring of activities in capital markets and sending alert signals when detecting anomalies. In Singapore, MAS has pushed forward technologies that analyse transactions reports and identify suspected cases of money laundering.<sup>59</sup>

While Suptech can enhance supervisory efficiency, human judgement is still required in onsite and offsite examinations to identify areas of vulnerabilities and to assess the potential risks in a forward-looking fashion. Table 4.2 highlights what can and cannot be performed by data analytics and AI technologies in supervision.

<sup>58</sup> RPA refers to software that can be easily programmed to do basic, repetitive tasks across applications. It is designed to reduce the burden of repetitive, simple tasks on employees.

<sup>59</sup> The Suptech use cases of ASIC and MAS are extracted from FSI Insights on *Innovative technology in financial supervision (Suptech) – the experience of early users*, BIS, July 2018.

**Table 4.2: What Suptech can and cannot do**

Can Do	+	+	+
Regulators can use Suptech to improve data collection such as (i) reporting, (ii) data management, and (iii) through virtual assistance.			
<p>Through the use of data analytic tools, regulators can obtain more insights by extracting information from various types of data for purposes of (i) market surveillance, (ii) misconduct analysis, and (iii) micro and macro prudential supervision.</p>			
Cannot Do	-	-	-
Banking supervisors need to investigate if irregular activities are detected, such as data gaps, potential breach cases and misconduct behaviour by banks.	-	Regulators still play an important role in communicating with bank management and risk officers to understand their operations and assess potential risks.	Suptech may not be able to identify potential risks based on data from different business areas of banks, such as the linkages between treasury operations and loan business.
<p>Forward-looking assessment and gathering market intelligence by supervisory agencies to guard against risks.</p>			

Source: HKIMR staff compilation.

#### 4.1.4: What are the prospects and limitations of using AI in Suptech?

Most Suptech initiatives are still at the development stage. According to the survey conducted by the Bank for International Settlements (BIS), about half of the 39 financial regulators in the sample have adopted explicit Suptech strategies or are at the planning stage, with less than a third operational.<sup>60</sup> Their findings suggest that data collection and analytics are the two key areas for Suptech applications. When the use of AI in Suptech matures, it will help regulators to (i) monitor risks using high-frequency accounting and loan data; (ii) identify misconduct or fraud cases by banks using big data and NLP; and (iii) detect irregular activities conducted by banks using AI.

While Suptech may offer new insights to regulators through enhanced data analytics, it also has limitations similar to other AI applications. For example, ML algorithms will have difficulties in detecting previously unknown forms of misconduct, anomaly and vulnerability.<sup>61</sup> If the ML algorithms and systems are not properly calibrated, Suptech may fail to identify potential risks arising from linkages between different operational areas (for example, treasury operations and the pattern of loans). Like the use of AI applications, the effectiveness of Suptech depends on the quality of the underlying data.<sup>62</sup> There are also legal risks that arise from handling a large amount of sensitive data.

The application of Suptech in public policy and decision-making can be limited by its opacity. Supervisors need to review irregular activities and misbehaviour detected by AI, as well as explain AI-driven decisions to stakeholders. More importantly, in order to benefit the

The use of AI in supervision, or Suptech, improves data collection and analytics, helping regulators gain additional insights from banks' structured and unstructured data in monitoring risks and detecting irregular activities.

most from Regtech and Suptech, regulators and banks need to work closely to establish mutually accessible interfaces to facilitate data and information exchange.

#### 4.1.5: HKMA initiatives on Regtech and Suptech

The initiatives on the Fintech Supervisory Sandbox (Sandbox) and the Sandbox Chatroom (Chatroom) have enabled banks and Fintech companies to seek the HKMA's regulatory feedback on smart banking and Fintech projects at the early stage.<sup>63</sup> The HKMA also recognises the growing need for and the development of a Regtech ecosystem in Hong Kong. To foster development in Regtech solutions, the HKMA has opened up the Sandbox and Chatroom to collect ideas on Regtech projects proposed by the banking industry and the Fintech community. The HKMA has also launched a series of Regtech related projects through its Banking Made Easy initiatives. These projects cover four areas summarised in Table 4.3.

<sup>60</sup> BIS (2019), *The Suptech Generations*, FSI Insights on Policy Implementation No. 19 (October).

<sup>61</sup> Gasparri, Giorgio (2019), *Risks and Opportunities of RegTech and SupTech Developments*, *Frontiers in Artificial Intelligence* Vol. 2 (July).

<sup>62</sup> Kuroda, Haruhiko (2017), *AI and the Frontiers of Finance*, Speech given by the Governor of the Bank of Japan at the Conference on AI and Financial Services/Financial Markets (Tokyo).

<sup>63</sup> The Fintech Supervisory Sandbox was launched by the HKMA in 2016 to allow banks and their partnering technology firms to conduct pilot trials of their Fintech ideas.

**Table 4.3: HKMA's policy initiatives in promoting Regtech and Suptech****AML/CFT Surveillance Technologies**

- Regtech solutions are increasingly being recognised as highly applicable in AML/CFT.
- The HKMA hosted the first AML/CFT Regtech forum in November 2019, which brought together some 400 participants including regulators, banks and other stakeholders.
- Experts in the Regtech sector sharing experience and identifying opportunities in applying technology to further enhance the effectiveness of AML/CFT efforts.

**Risk Management and Compliance**

- The HKMA has been observing a diverse range of local and overseas Regtech use cases, and considered that it would be helpful to share these observations with the banking industry.
- To this end, the HKMA launched a newsletter series, the *Regtech Watch*, in November 2019 to share observations about Regtech use cases in various areas with the industry, to facilitate the use of Regtech by the banking sector.

**Machine-readable Regulations**

- The HKMA is conducting a deep-dive study on the needs for, and possibilities of, machine-readable regulations for selected regulatory requirements.
- The study will provide better insights on whether machine-readable regulations are desirable and feasible in Hong Kong.

**Suptech in Banking Supervision**

- The HKMA is exploring the use of Suptech to enhance its effectiveness and forward-looking capability.
- The targets include further automating its interactions with banks, including:
  - Streamlining banks' regulatory data collection mechanism;
  - Enhancing digitalisation and analytics of supervisory information;
  - Automation of supervisory processes.

Note: CFT refers to counter-financing of terrorism.

Sources: HKMA and HKIMR staff compilation.

The HKMA is planning to introduce additional Regtech-related initiatives. A common objective of these initiatives is to identify challenges facing the banking industry throughout the regulatory compliance journey and build a larger and more diverse Regtech ecosystem. The HKMA is taking a leading role in facilitating this important component of the Smart Banking era. With closer collaboration among the banking industry, the technology community and the HKMA, the successful adoption of Regtech and Suptech can offer tremendous potential to complete the Smart Banking ecosystem in Hong Kong.

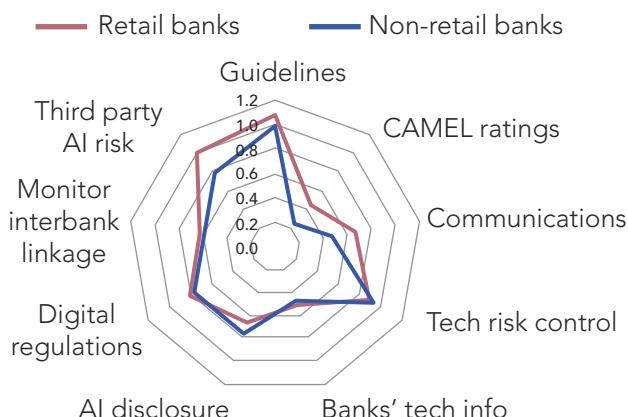
To explore further use of Regtech and Suptech, the HKMA has rolled out new initiatives on using AI to enhance AML surveillance, risk management, compliance and supervisory capacity.

## 4.2: ROLE OF POLICYMAKERS IN FOSTERING AI DEVELOPMENT IN BANKING

Despite challenges and risks, most banks believe that integrating AI technologies into their businesses will improve efficiency and services to customers. In promoting financial innovations through the further use of AI, it is important for policymakers to provide a conducive environment and transparent supervisory framework for AI adoption. In the HKMA AI Survey, where banks were asked about what regulators could do to foster AI development in Hong Kong, both retail and non-retail banks highlighted the importance of clear guidelines and regulatory requirements on technology risk management (Chart 4.1). In response, the HKMA issued *High-level Principles on Artificial Intelligence* in November 2019 to provide general guidelines for banks in managing risks associated with using AI applications.

**Chart 4.1: Regulatory issues that banks most support**

(score: higher=greater support)



Source: HKIMR staff calculations based on the HKMA AI Survey.

In response to the key challenges including development, technical and regulatory issues faced by banks in developing AI applications, policymakers may take the lead to strengthen public-private co-operation to provide support to banks in developing new AI applications. For development issues concerning talent scarcity and for technical issues on the complexity of model design and validation, one possible solution is to establish a public-private sector working group to promote knowledge exchange and experience sharing. To achieve this, a range of events could be organised with the support of policymakers. Examples of events may include the following:

- **Workshops:** these events may be used to demonstrate the basic building blocks of AI models, the application of ML algorithms and programming techniques in the development of new AI applications;
- **Seminars:** industry leaders or speakers with good knowledge and experience in data science, ML and AI may be invited to share the latest developments in using AI in banking, and to discuss the latest techniques in model design and validation;

- **Presentations:** knowledge experts from the private and public sectors and the academia may be invited to speak on topics of common interest; and
- **Supporting platform:** an online platform may be set up for banking practitioners to seek advice and solutions from experts in data science and AI for developing in-house models.

To encourage participation from people with keen interests in developing AI applications in banking, the public-private working group could invite experts from banks, Fintech companies, data specialists, IT consultancy firms and universities to join these events. This will help bridge the gap between the users and developers of AI models. Over the longer term, banks may work with universities to design programmes on data science and AI applications to enhance the relevant skillsets of fresh graduates in this area. To foster financial innovation such as broader use of AI by banks, the HKMA introduced a Fintech Supervisory Chatroom within the Fintech Supervisory Sandbox in 2017 to provide supervisory feedback to banks and tech firms at the early stages of their Fintech projects.

On regulatory issues, the rapid expansion of AI adoption by banks has inevitably created legal gaps that need to be addressed to avoid stifling innovation. The HKMA AI Survey shows that uncertainty about compliance risks and legal consequences of using AI is a key concern for banks in taking further steps to develop and deploy new AI applications. As more new AI models are adopted by banks, regulators will consider providing further guidelines on the use of AI technologies by banks as necessary.

**Policymakers can play a role in strengthening public-private co-operation by organising forums where participants from banks, Fintech firms, data specialists and universities can interact.**

# CONCLUSIONS

---

60

The use of AI in banking is growing and becoming more broad-based, underpinned by enhanced computational capacity, advanced data analytics and maturity in machine learning algorithms. The findings from the HKMA AI Survey show that banks in Hong Kong are aware of the risks and challenges of integrating AI into their businesses, but these will not hinder further use of AI as banks benefit from efficiency gains and cost reductions. **Banks seeking to enhance competitiveness through financial innovations will utilise AI as a way of accomplishing this objective.**

New technologies require new tools for managing the risks of using AI models, which comprise three key components including data input, model design and validation. **Banks may put in place a robust governance framework to oversee and mitigate the risks associated with data quality and security, and to detect possible faults in model design through rigorous validation procedures.** Cybersecurity of AI systems and cloud computing need to be strengthened in the face of new cyber threats. Tackling these risk management challenges requires clear objectives and direction from senior management, good communication with major stakeholders and deployment of adequate resources.

For regulators, there are two key considerations in supervising the adoption of AI by banks. **One is seeking to balance the objectives of maintaining financial stability, upholding consumer protection and nurturing innovation, and the other is exploring the potential application of AI in compliance and supervision.** To foster AI development with a proper oversight of the risks, financial regulators around the globe have set out guiding principles to promote a sound, fair and prudent use of the technology.

Policy initiatives in facilitating the use of AI in compliance and supervision can benefit both banks and regulators. Banks have expanded the use of Regtech in data submission, regulatory reporting and fraud detection. Regulators have made use of Suptech to gain direct access to banks' data through API, extracting new insights from various types of data. **To achieve greater synergies from using Regtech and Suptech, banks and regulators may work together to explore the best use of AI in compliance and supervision,** such as introducing machine-readable regulations and enhancement of data infrastructure.

Advancements in AI technology and its broader use in banking will create new opportunities and pose new challenges to banks and regulators. **To overcome the challenges faced by banks, such as talent scarcity and difficulty in validating AI models, policy initiatives in strengthening public-private co-operation can help to promote knowledge exchange and experience sharing.** Regulators will explore AI technologies and data science to cope with the increased complexity of AI models used by banks, and remain vigilant to the potential systemic impact of the broader use of AI on financial stability.

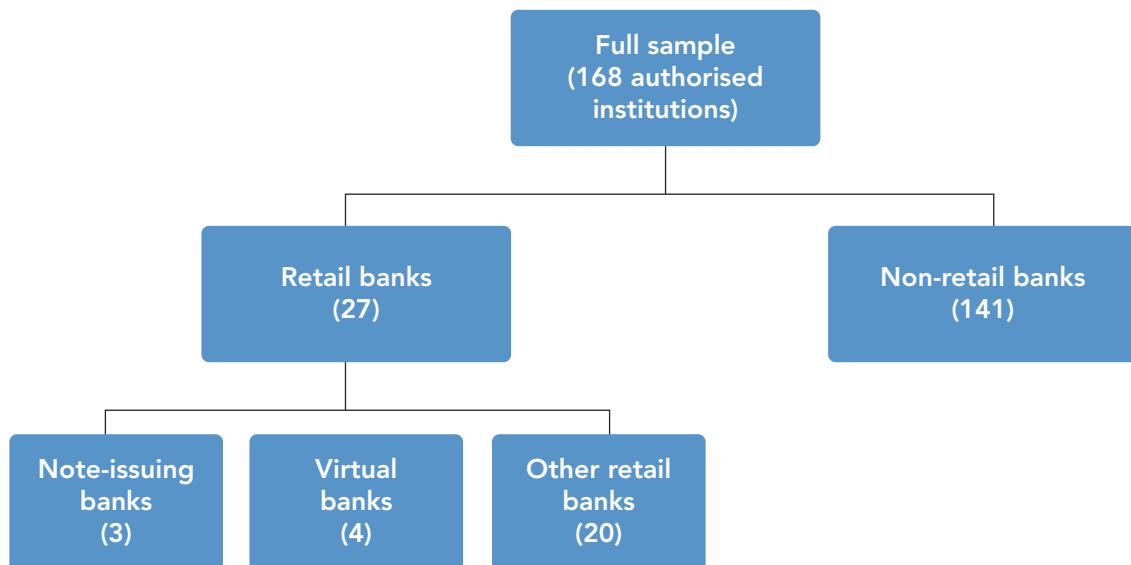
# APPENDIX A: BACKGROUND OF THE HKMA AI SURVEY

The results presented in this report are based on the findings from a survey on the *Application of Artificial Intelligence Technology in the Banking Industry* conducted by the HKMA in August 2019. The FFO and the Banking Supervision Department of HKMA designed the questions in the survey, in consultation with the HKIMR and the Chinese University of Hong Kong. PwC, the FFO, the Banking Supervision Department of the HKMA and the HKIMR participated in the interviews with banks and Fintech companies to gather insights from market practitioners on AI adoption in Hong Kong.

The survey was conducted to collect information about the current status of AI adoption by authorised institutions in Hong Kong, including the types of AI applications that authorised institutions have adopted or plan to launch, the amount of resources (e.g., manpower and capital) deployed in developing AI applications, and the reasons for and benefits of integrating AI into the business models of authorised institutions.

Furthermore, the challenges and potential risks arising from the broader use of AI technologies, as well as ethical, governance and regulatory issues were also covered in the survey.

A total of 168 completed questionnaires have been received from authorised institutions, including 27 retail banks and 141 non-retail banks. Among the retail banks, three of them are note-issuing banks and four of them are virtual banks. Non-retail banks mainly include Mainland banks and foreign bank branches in Hong Kong. The number of respondents vary across different questions in the survey.



# APPENDIX B: REFERENCES

---

**Bank for International Settlements/BIS (2018):** "Innovative technology in financial supervision (suptech) — the experience of early users" FSI Insights No.9, July (Broeders D and J Prenio).

**Bank for International Settlements/BIS (2019a):** "Big tech in finance: opportunities and risks" Chapter III of BIS Annual Report, June.

**Bank for International Settlements/BIS (2019b):** "The suptech generations" FSI Insights No.19, October (di Castri, S, S Höhl, A Kulenkampff and J Prenio).

**Bank of England/BoE (2019a):** "Machine learning in UK financial services", October.

**Bank of England/BoE (2019b):** "Outsourcing and third-party risk management" Consultation Paper CP30/19, December.

**Bank of England/BoE (2020):** "Transforming data collection from the UK financial sector", January.

**Basel Committee on Banking Supervision/BCBS (2018):** "Sound practices: implications of fintech developments for banks and bank supervisors", February.

**Basel Committee on Banking Supervision/BCBS (2019):** "Report on open banking and application programming interfaces", November.

**Brainard L (2018):** "What are we learning about Artificial Intelligence in financial services?" Speech at Fintech and the New Financial Landscape, Philadelphia, Pennsylvania, 13 November.

**Bundesanstalt für Finanzdienstleistungsaufsicht/BaFin (2019):** "Big data meets artificial intelligence: challenges and implications for the supervision and regulation of financial services".

**Croxson S, P Bracke and C Jung (2019):** "Explaining why the computer says "no"" FCA Insight, May.

**Deloitte (2019):** "The Evolution of Model and Algorithmic Risk: A Robust Model Risk Management Framework for Financial Institutions".

**De Nederlandsche Bank/DNB (2019):** "General principles for the use of Artificial Intelligence in the financial sector" (J van der Burgt).

**Dobeck, M (2017):** "A cybersecurity framework: Six steps to empowering your analytics", Cleveland State University College of Business.

**European Central Bank (2019):** "ECB Guide to Internal Models", October.

**European Commission (2020):** "Robustness and Explainability of Artificial Intelligence" JRC Technical Report (Hamon R, H Junklewitz and I Sanchez).

**Falk, M (2019):** "Artificial intelligence in the boardroom." FCA Insight, August.

**Federal Bureau of Investigation/FBI (2020):** "2019 Internet Crime Report", February.

**Federal Reserve (2011):** "Supervisory Guidance on Model Risk Management", April.

**Financial Conduct Authority/FCA (2019):** "Digital Regulatory Reporting: Pilot Phase 1 Report".

**Financial Stability Board/FSB (2019):** "Big tech in finance: market developments and potential financial stability implications", December.

**Gasparri G (2019):** "Risks and Opportunities of RegTech and SupTech Developments", *Frontiers in Artificial Intelligence* Vol. 2, July.

**General Data Protection Regulation/GDPR:** GDPR Enforcement Tracker.

**Heaven D (2019):** "Why deep-learning AIs are so easy to fool: Artificial intelligence researchers are trying to fix the flaws of neural networks" *Nature*, 9 October.

**Hong Kong Monetary Authority/HKMA (2016a):** "Risk-based and technology-neutral — the HKMA's supervisory approach to financial technology (Fintech)" *inSight*, March.

**Hong Kong Monetary Authority/HKMA (2016b):** "Cybersecurity Fortification Initiative", 21 December.

**Hong Kong Monetary Authority/HKMA (2019a):** "High-level principles on artificial intelligence", 1 November.

**Hong Kong Monetary Authority/HKMA (2019b):** "Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions", 5 November.

**Hong Kong Monetary Authority/HKMA (2019c):** "Reshaping banking with artificial intelligence", December.

**Institute of International Finance/IIF (2019):** "IIF machine learning recommendations for policymakers", September.

**Kuroda, H (2017):** "AI and the Frontiers of Finance," Speech given by the Governor of the Bank of Japan at the Conference on "AI and Financial Services/Financial Markets", Tokyo.

**Manyika J, J Silberg and B Presten (2019):** "What Do We Do About the Biases in AI?" *Harvard Business Review*, 25 October.

**Marr B (2018):** "The AI Skills Crisis And How To Close The Gap" *Forbes*, 25 June.

**McKinsey (2017):** "The Evolution of Model Risk Management", 10 February (Crespo I, P Kumar, P Noteboom and M Taymans).

**McKinsey (2019):** "The risk-based approach to cybersecurity", 8 October (Boehm J, N Curcio, P Merrath, L Shenton and T Stahle).

**Monetary Authority of Singapore/MAS (2018):** "Principles to promote fairness, ethics, accountability and transparency in the use of artificial intelligence and data analytics in Singapore's financial sector", November.

**Office of the Government Chief Information Officer, HKSAR Government (2018):** "Practice Guide for Cloud Computing Security", July.

**OpenText Corporation (2018):** "AI in Financial Services: Next Steps to Realising the Potential", April.

**Proudman, J (2019):** "Managing machines: the governance of artificial intelligence." Speech at FCA Conference on Governance in Banking, 4 June.

**Restoy, F (2019):** "Regulating fintech: what is going on, and where are the challenges?" ASBA-BID-FELABAN XVI Banking public-private sector regional policy dialogue "Challenges and opportunities in the new financial ecosystem." Washington DC, 16 October.

**SAS Institute (2017):** "10 Mistakes to Avoid When Launching Your Data Governance Program" SAS Institute White Paper (Dyche J and K Nevala).

**SAS Institute (2018):** "The SAS Data Governance Framework: A Blueprint for Success" SAS Institute White Paper.

**van Steenis, H. (2019):** The future of finance: a report for the Bank of England, 20 June.

## **ABOUT THE HONG KONG ACADEMY OF FINANCE (AoF)**

The AoF is set up with full collaboration amongst the HKMA, the Securities and Futures Commission, the Insurance Authority and the Mandatory Provident Fund Schemes Authority. By bringing together the strengths of the industry, the regulatory community, professional bodies and the academia, it aims to serve as (i) a centre of excellence for developing financial leadership; and (ii) a repository of knowledge in monetary and financial research, including applied research.

## **ABOUT THE HONG KONG INSTITUTE FOR MONETARY AND FINANCIAL RESEARCH (HKIMR)**

The HKIMR is the research arm of the AoF. Its main remit is to conduct research in the fields of monetary policy, banking and finance that are of strategic importance to Hong Kong and the Asia region. The Applied Research studies undertaken by the HKIMR are on topics that are highly relevant to the financial industry and regulators in Hong Kong, and they aim to provide insights on the long-term development strategy and direction of Hong Kong's financial industry.

### **CONTACT US**

Email: [hkimr@hkma.gov.hk](mailto:hkimr@hkma.gov.hk)

Tel: +852 2878 1706

Website: <https://www.aof.org.hk/research/HKIMR>