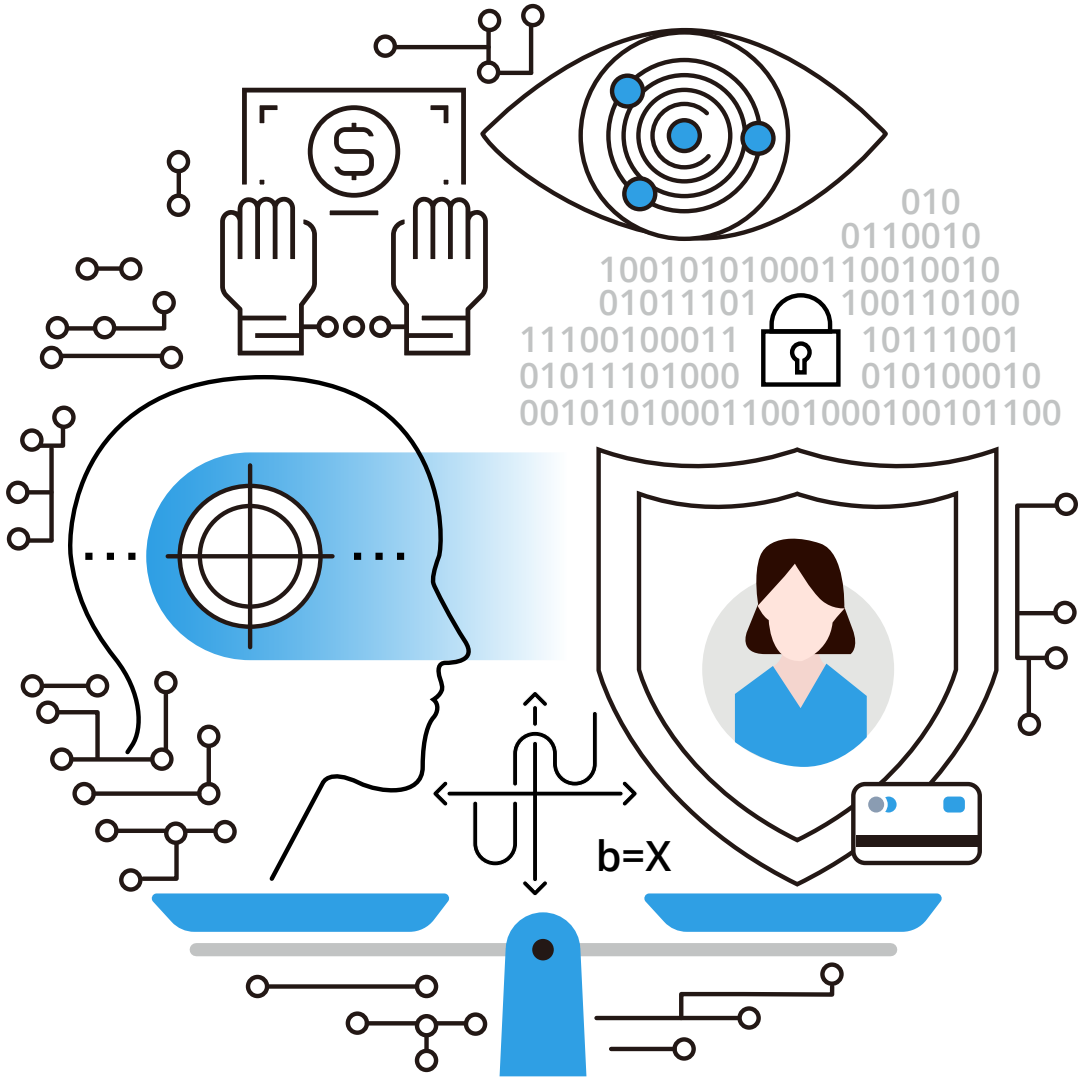
Deloitte.



Centre for Regulatory Strategy

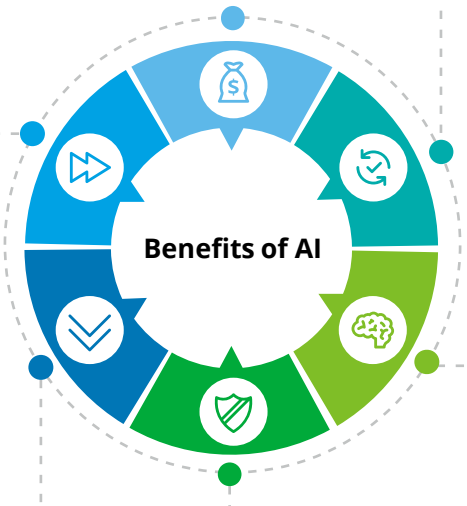
Trustworthy Use of Artificial Intelligence in Finance

Regulatory Perspectives from Asia Pacific

Introduction

The digital evolution of the financial services (FS) industry is heavily reliant on having quality information and analytics to deliver services to customers and manage operations in an efficient and risk-appropriate manner. With developments in Artificial Intelligence (AI) transforming the information processing and data analytics landscape, and opening up potential benefits, such as business process simplification, cost reduction, efficiency improvements and enhanced customer engagement, FS firms have become early adopters of AI. According to a 2022 survey among global FS firms conducted by a technology service provider, 78% of respondents indicated that they are using at least one form of AI,[1] including machine learning, deep learning, and high-performance computing (HPC). For the purpose of this paper, we define AI as a branch of computer science that explores the simulation of human cognitive functions such as learning and problem-solving. We will discuss AI primarily from a regulatory perspective, covering key AI-related principles enunciated by Asia Pacific (AP) regulators, their implications for FS firms in the region, and what FS firms need to do to address the concerns of regulators and customers.

Figure 1: Benefits of AI Applications in the FS Sector



Cost Reduction

Applying AI and intelligent solutions to automate tasks that are repetitive can reduce, hence reducing costs through improved efficiency and quality.

Example:
Conducting Anti-Money Laundering (AML) and Know Your Customer (KYC) through AI-driven solutions to reduce resource spent on completing these tasks manually.

Faster execution

Reducing the time required to achieve operational and business results by minimising latency.

Example:
Using AI-driven real-time fraud detection to block fraudulent activities in a more timely manner.

Reduced complexity

Recognising patterns in increasingly complex sources and improving decision making and through analytics that are more effective and predictive.

Example
Leveraging non-traditional data sources, such as social media, to detect potential money laundering or terrorist financing activities.

Transformed engagement

Enabling technology-empowered products to communicate with customers with a human touch, rather than forcing customers to understand the machine language.

Example:
Using conversational bots that can capture and respond to customer sentiments to address customer needs more effectively.

Fueled innovation

Enhancing competitive advantage by using AI to enable innovative new products, identify new markets, and develop new business models.

Example:
Recommending new FS products based on customer needs and preferences through data analytics.

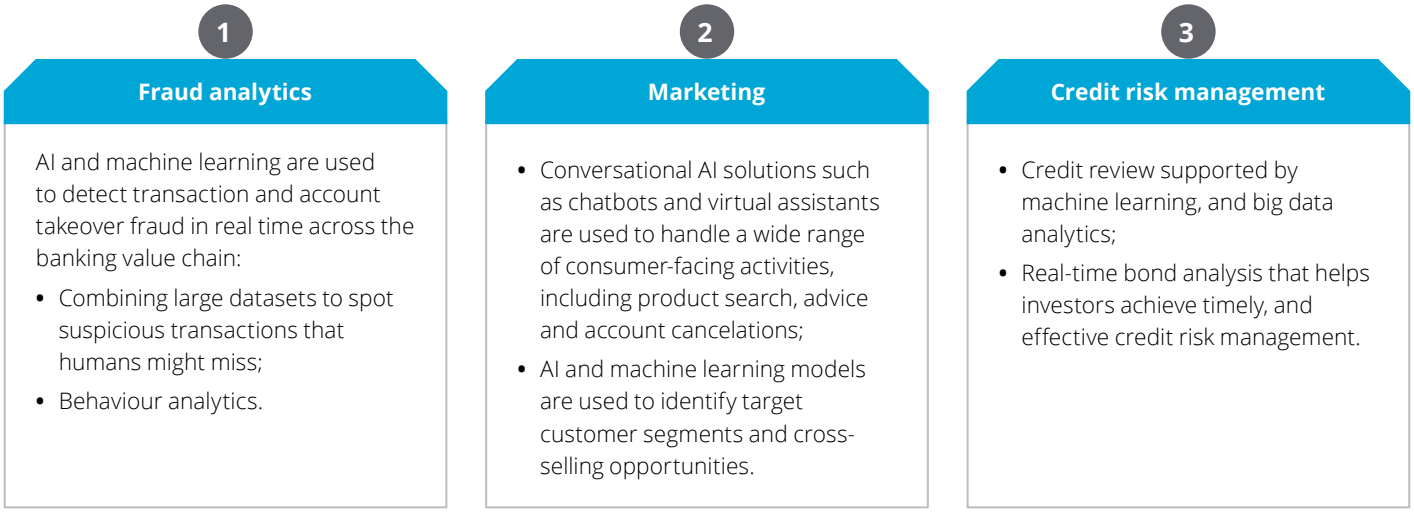
Fortified trust

Securing business from fraud and cyberattacks. Improving product and service quality while enabling greater transparency to enhance brand trust.

Example:
Identifying and getting prepared for cyber-attacks and data breaches before they occur.

Based on our work with clients, the most commonly used AI applications in the FS sector in the AP region include fraud detection, marketing, and consumer onboarding (including assessing money laundering risk). AI has also been adopted by banks as part of the credit analysis process, by insurers to process claims and improve the underwriting process, and by asset management firms to automate trade operations and provide market insights to clients.

Figure 2: Examples of use cases of AI in the FS sector



While many FS firms have already embarked on the journey of AI deployment, challenges remain. According to our observations, two of the biggest issues facing FS firms with regard to the use of AI are:

1) achieving accurate and satisfactory results that meet business objectives; and
2) incorporating risks associated with the use of AI in FS firms' risk management frameworks and managing the risks appropriately.

At the root of the first issue is the fundamental difference between rules-based analytics, which is conducted with predetermined formulas and algorithms, and AI-based analytics, which is a self-learning process using training data. The pre-determined nature of rules-based analytics makes it easier for stakeholders to understand, implement, and modify. In comparison, AI analytics has the potential to provide greater insights and wider coverage, especially when a large number of variables are involved. However, AI applications are complicated, difficult to explain, and require a comprehensive understanding of both the business context and the AI technology to implement and achieve accurate results that serve business needs.

The second issue arises from the lack of awareness of the risks associated with AI applications in the FS sector, and the absence of risk management frameworks to properly address them. For example, the legal and reputational risks stemming from potential AI-induced discrimination on the grounds of sex, race, age, disability, or national origin of FS customers. These risks and their increasing threat to consumer protection have come into the focus of financial regulators and lawmakers across jurisdictions.

In the AP region, the Monetary Authority of Singapore (MAS) was among the first regulators to issue a set of principles to promote fairness, ethics, accountability, and transparency (the *FEAT Principles*) in the use of AI and data analytics in finance,[2] followed by a thematic review on a selected group of banks and insurers in 2021.[3] Other AP regulators, such as the Hong Kong Monetary Authority (HKMA) and South Korea Financial Service Commission (FSC), have also released high-level guidelines in recent years to assist FS firms to understand, evaluate and mitigate risks associated with the growing use of AI across the sector. Other jurisdictions, such as Australia[4] and China mainland,[5] have adopted AI-related ethics principles issued by either the government or cross-sectoral regulators, with FS sector-specific regulation under discussion.

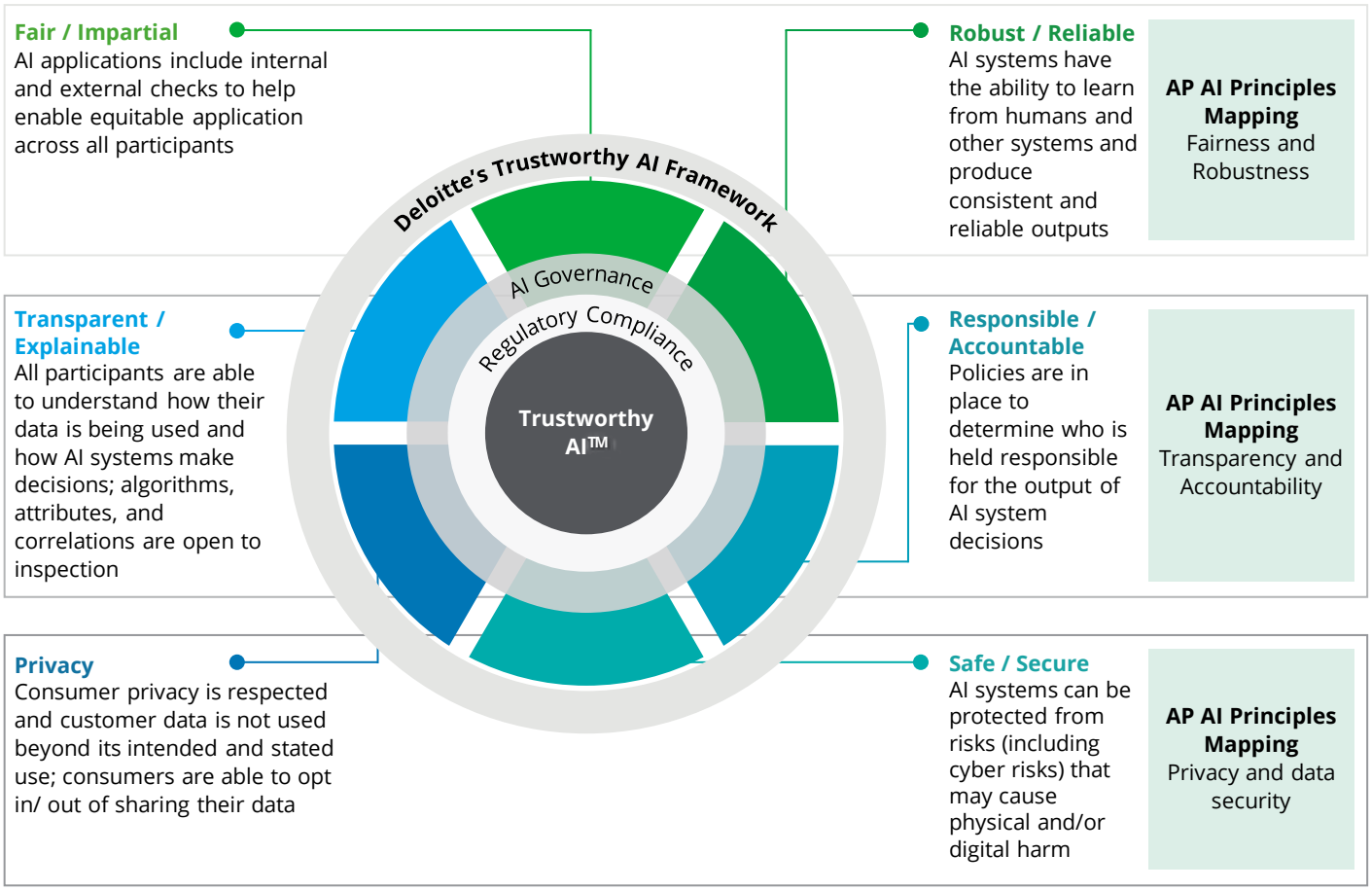
Figure 3: Examples of AP AI Principles compared to the EU Ethics Guidelines for Trustworthy AI

Key elements	European Union	Singapore	Hong Kong SAR	South Korea	Australia
Robustness	Technical robustness and safety	Accuracy	Sufficient expertise, explainability and good data quality	Accuracy and safety	Reliability and safety
Fairness	Diversity, non-discrimination and fairness	Justifiability	Fairness	Fairness	Fairness
		Bias		Consumer rights	
					Human values
Accountability	Accountability	Internal accountability	Governance and accountability	Responsibility	Accountability
		External accountability	Auditability, model validation and third-party oversight	Equivalent level of safety and security for third-party contractors	
Transparency	Transparency	Transparency	Transparency and disclosure	Transparency	Transparency and explainability
			Develop strategic recommendations		Contestability
Privacy and data security	Privacy and data governance		Data privacy and protection		Privacy protection and security
Human oversight	Human agency and oversight				
Social and environmental wellbeing	Societal and environmental wellbeing	Ethics			Human, societal and environmental wellbeing

In Figure 3 we compare the AI principles issued by some AP regulators to the *EU Ethics Guidelines for Trustworthy AI*.[6] We have identified seven common elements across these AI principles: robustness, fairness, accountability, transparency, privacy and data security, human oversight, and social and environmental wellbeing. In general, the key elements covered are similar across different regions. The *EU Ethics Guidelines for Trustworthy AI* explicitly covers human oversight as well as social and environmental principles in the framework. While the only AP AI framework that calls out human oversight and social and environmental wellbeing is *Australia's AI Ethics Framework*,[7] the majority of the AP financial regulators have addressed these elements indirectly by requiring FS firms to comply with relevant laws and regulations and to adopt sound ethical standards.

These regulatory principles map closely to Deloitte's Trustworthy AI Framework, which sets out what an effective AI governance framework should look like.[8] The Deloitte framework covers six key elements: fairness, robustness, transparency, data privacy, accountability, and security.

Figure 4: The elements of the AP AI principles mapped to the Deloitte Trustworthy AI Framework



Transparency and accountability

A key concern shared among regulators is the 'black box' nature of AI, as well as the challenge to hold FS firms accountable for the decisions made based on AI-produced results. As noted above, AI applications are not built based on fixed predetermined rules, which can be interpreted by explaining what the rules, variables, and data inputs are. Instead, AI, as defined in this report, rely on training data and live data inputs, the outputs from which are therefore more challenging to explain to internal users of the AI applications, and even more so for external stakeholders. To address this issue, the transparency and explainability principles require FS firms that have adopted AI applications to ensure an appropriate level of transparency and disclosure of the models and how they may impact customers. For example, when the AI model suggests a premium increase for an insurance policyholder based on their lifestyle, the insurer using the AI application should be able to explain to the policyholder why, and how, this lifestyle is contributing to the premium increase. The specific regulatory expectations on transparency and explainability vary across jurisdictions. The HKMA requires FS firms to put in place a mechanism for customers to request reviews of the decisions made by AI applications.[9] In its *FEAT Principles*, MAS discusses the costs and benefits of disclosing technical details of AI applications and concludes that clear explanations of the decision-making process should be provided to impacted parties upon request, without revealing the proprietary component of the AI applications.

Australia's AI Ethics Principles recommend an additional dimension to explainability, which is the contestability of the AI applications. The contestability element requires that firms using AI applications to give recommendations provide an avenue for the impacted parties to contest the recommendations. This requirement enables customers to interact with the AI process to challenge certain points in decision-making.[10] The contestability element is closely linked to the explainability principle. For example, when an AI decision is challenged by the impacted party, the decision needs to be clearly explained to make sure all parties involved in the decision understand how the outcome was derived.[11]

Transparency is important not only for the fair treatment of customers but also for achieving satisfactory results within the business context. The Organisation for Economic Co-operation and Development's (OECD) *2019 AI Principles* indicated that proper disclosure should be made to all stakeholders who have interactions with AI systems.[12] In other words, stakeholders need a clear understanding of how the results are produced by the AI applications to make informed decisions. This can include those working with AI applications in a front office capacity offering products to customers, those underwriting risks based on AI model results, risk management teams using AI applications to predict default rates and calculate provisions, and internal control teams ensuring compliance with laws and regulations.

Risk-tiering and the materiality assessment

Transparency and explainability are more important for some AI applications than others, depending on the use cases. For example, pricing applications tend to require a higher level of transparency and explainability than AML or fraud applications. The decision-making process of the pricing applications has a direct impact on a large group of customers and a lack of transparency poses higher legal and reputational risks to the FS firm, on the other hand, increased transparency on the AML or fraud detection applications might hinder their ability to serve their purpose. For this reason, some regulators have set out guidelines on implementing AI-related principles using a risk-tiering approach that takes into account the materiality of the applications. One example of this approach is the proposed EU *Artificial Intelligence Act*, which categorises AI applications into three risk groups: unacceptable risk applications, high-risk applications, and other non-high-risk applications.[13] Different requirements are proposed for specific AI applications, commensurate with their level of risk. In the MAS *FEAT Principles*, the materiality of the AI application is also taken into account in the implementation guidance of each principle.

The accountability principle enhances the transparency principle by requiring FS firms to adopt governance frameworks that clearly define responsibilities of oversight, validation and approval throughout the life cycle of an AI application. Within the FS firm, the Board of Directors and Senior Management should be made aware of AI-related risks and key staff members should be assigned to fully understand and oversee the AI applications, as well as to approve decisions made based on AI. Whenever a third-party is involved, the FS firm should be accountable for the AI applications produced by the third-party. Externally, proper channels for customers to inquire about the AI decision-making process should be provided.

What firms can do to align with the transparency and accountability principles

An effective governance framework supporting transparency and accountability is as important as proper modeling techniques when developing AI applications. FS firms should strike a balance between model complexity and explainability, and adopt a comprehensive governance framework, covering all business functions of the firm, that defines and documents the responsibilities of risks associated with AI applications.

FS firms using AI applications should consider the following:

1) Ensuring all stakeholders (across all levels of the business) using AI applications understand how the AI applications work, and how to interpret the results. This includes the Board of Directors and Senior Management, who are responsible for ensuring transparent, accurate, and ethical results of the AI application.
2) Define responsibilities and accountability for risks associated with AI applications in the risk management framework. The Board of Directors and Senior Management should be aware of the AI applications and their risks.
3) Establish a set of criteria to distinguish between information that should be disclosed to customers and information protected by intellectual property rights.
4) Establish a mechanism for proactive communications and response upon request to disclose the decision-making process of the AI applications to the extent that is useful and understandable for customers.
5) When contested by customers, a mechanism should be in place to revisit the decisions made by the AI application.

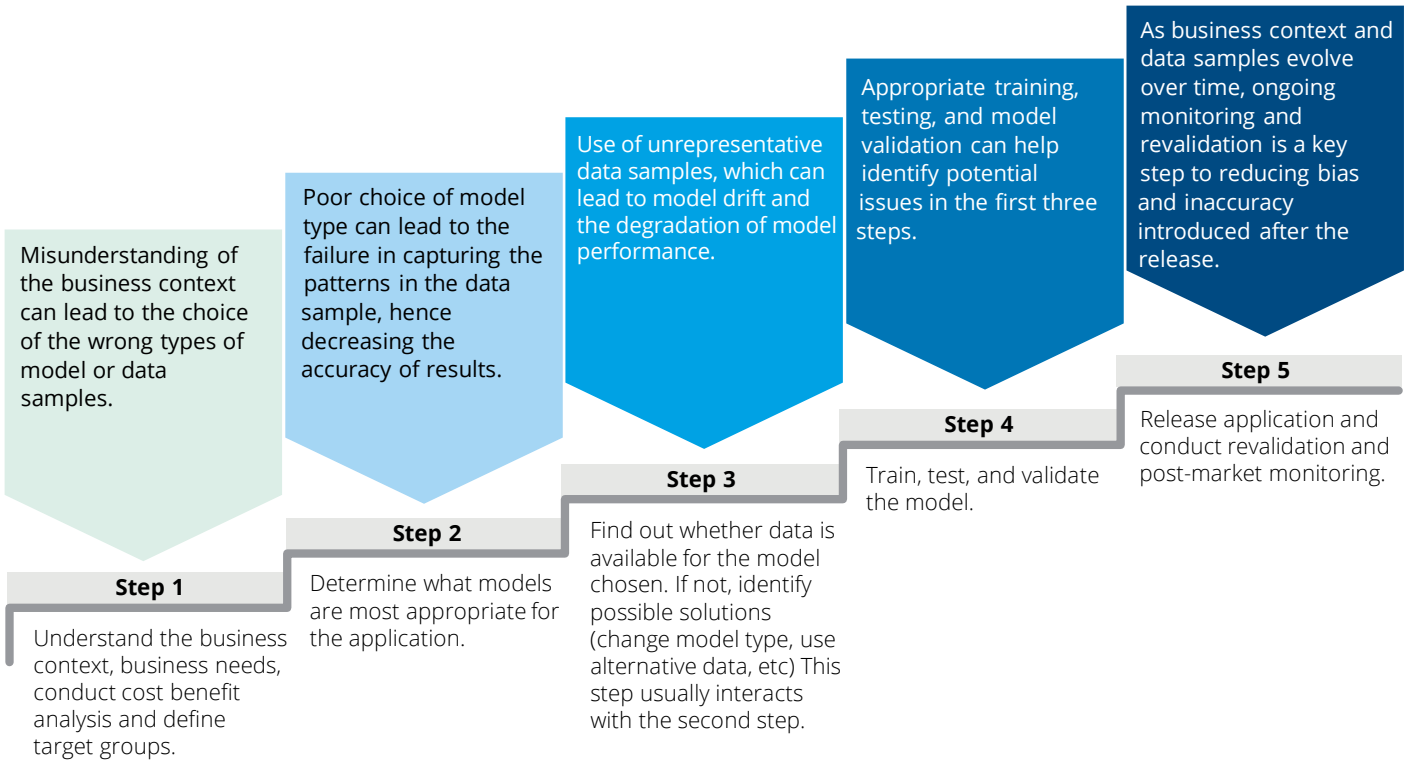
Fairness and robustness

Another key concern of regulators focuses on protecting customers from potential discrimination and other unfair treatment. Because a large amount of personal data is collected from customers as training data and model inputs, how this data is collected and used may have a significant impact on the products and services offered and/or provided to customers. What lies at the core of fairness is that the results produced by AI, which are then used to make decisions for customers, need to be accurate and unbiased. The principle on robustness is therefore closely linked with the principle on fairness. Principles on fairness and robustness generally revolve around three aspects:

- Firstly, AI applications in the FS sector should be inclusive and should not systematically discriminate against certain individuals or groups. Whenever personal attributes are used, it should be justifiable;[14]
- Secondly, recommendations made based on AI applications should be "fit and proper" for the customer's situation;[15] and
- Thirdly, the models used in AI applications should be robust, accurate and unbiased.[16]

A key challenge in implementing the fairness principle is identifying and eliminating model bias, which is a long-standing issue in the use of AI and can sometimes lead to unfair treatment of customers. The cause of model bias is complicated – there are a number of factors contributing to biased results, and model bias can be introduced in any of the five steps of model development, as outlined in Figure 5 below:

Figure 5: Five steps to unbiased and accurate results in the AI application development process



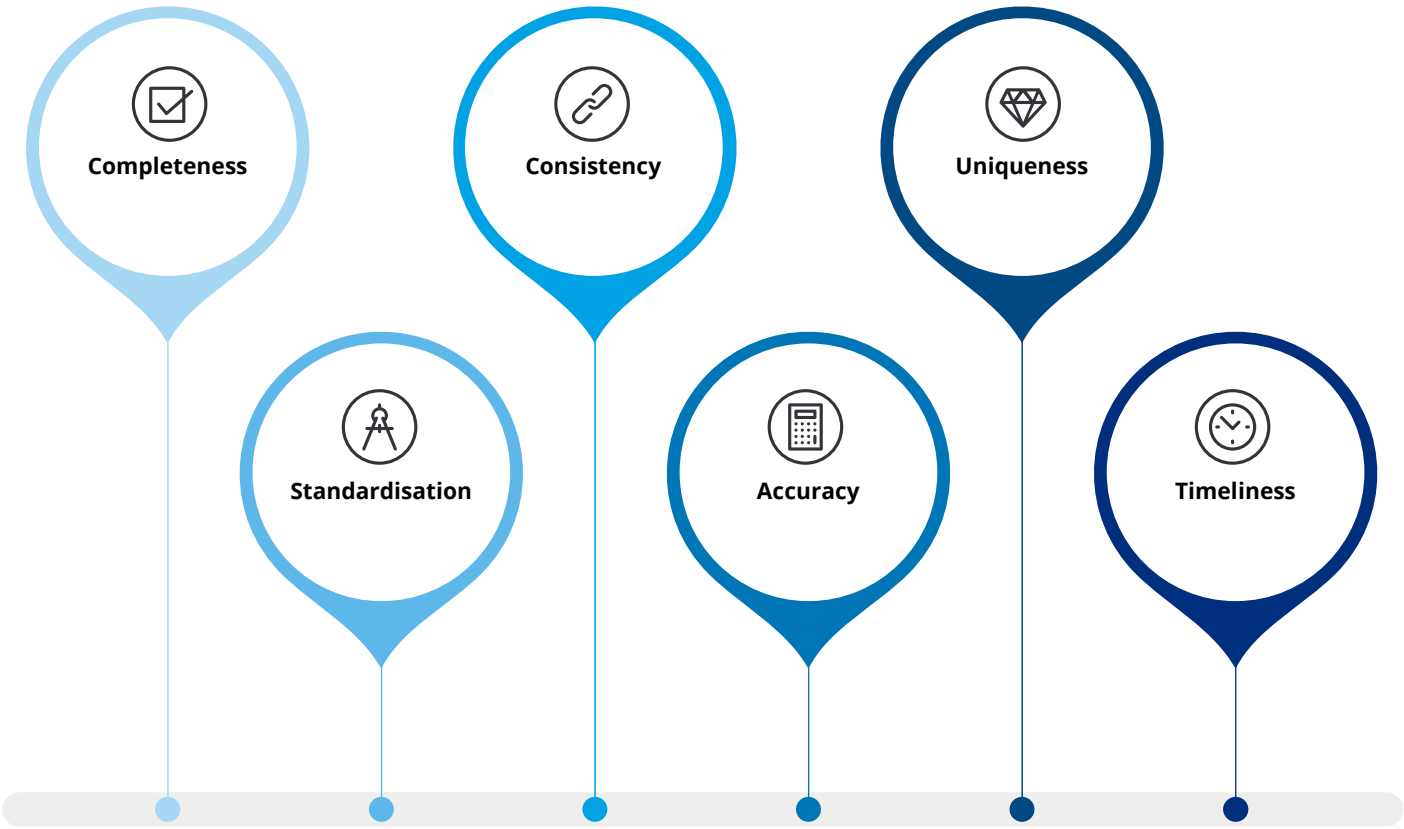
Insufficient understanding of the business context can lead to poor model selection, which then impacts the accuracy of the results. Models are trained by data; therefore, non-representative training data will create biased models. In addition to these two key steps, biased results can also be produced as a result of poor model calibration, use of a poor sampling scheme, or the lack of ongoing monitoring and re-validation.

Among the above factors contributing to model inaccuracy and bias, data quality plays the most important role. For example, the use of non-representative training data, imbalanced data inputs, as well as the use of ambiguous data could all lead to degradation of model performance and subsequently inaccurate or biased model results. Another example is the challenge of incident labeling in AML applications. In some jurisdictions, the lack of data on money laundering incidents to use as labels or identifiers creates challenges for building AI applications for AML purposes.

AI principles in most jurisdictions specifically require FS firms adopting AI applications to be accountable for the quality of data, to ensure the robustness of AI applications. Both the MAS *FEAT Principles* and the HKMA *High Level Principles on Artificial Intelligence* require FS firms to conduct data quality assessments as well as regular reviews and validation of their data.[17, 18] In order to comply with these data quality requirements and enhance the fairness and robustness of AI applications, FS firms should conduct data quality assessments on elements such as:

1) Completeness: checking whether there are gaps of information in the data.
2) Standardisation: harmonising the format of data being used
3) Consistency: harmonising the view of data.
4) Accuracy: ensuring the data used capture information correctly.
5) Uniqueness: avoiding multiple entry of the same data point.
6) Timeliness: ensuring timely capture of information.

Figure 6: Six elements of data quality assessment



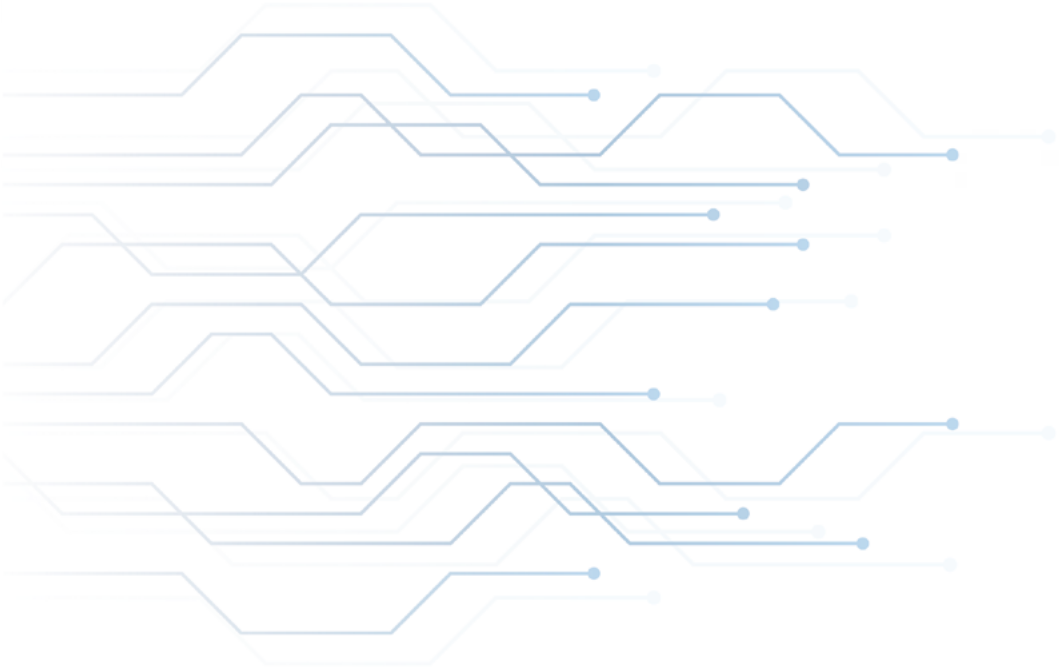
What firms can do to align with the fairness and robustness principles

1) Defining business context and performing validation:
   - AI systems often include more than mathematical models and data; business context and human judgment are also key components of the AI model to avoid bias and ensure ethical practices.
   - Adopt effective model performance and fairness checks for AI application evaluation.
   - Data quality assessments should be conducted on a regular basis and as part of the data governance framework, capturing all important aspects of data quality.
   - Strengthening the data management framework, and upgrading IT infrastructure to improve data quality at the source.
   - Considering alternative sources of data or alternative model types when data quality is deemed insufficient.

2) Ongoing monitoring:
   - Embed fairness assessments into the AI system development lifecycle. Formally define fairness metrics with diverse representation in the consultation process to ensure fairness is encoded and measured throughout development pipeline, prior to deployment.
   - Develop criteria, standards, and/or metrics that can measure the extent to which commitments have been met.
   - Incorporate the concepts, principles and commitments into policies and procedures of the firm's operations and the AI model governance framework to make justifiable decisions.

3) Carefully design and implement process controls to ensure AI applications do not introduce unintended risks and harms in the data driven decision-making processes.

4) Adopt both In-time validation (at model development state) and periodic out-of-time validation (throughout the model's life cycle).



Privacy and data security

The privacy and data security principles are the fundamental building blocks of a safe AI application and are not exclusive to the use of AI in finance - they apply to all firms that collect, transmit, and store personal data. While AI-related regulations are still at a nascent stage in many AP jurisdictions, data privacy laws and regulations are more mature. Ensuring compliance with data protection laws in the life cycle of AI applications is key to fulfilling the privacy and data security principles.

In some jurisdictions, alternative data sources such as social media data or third-party data are used in AI applications when internal data is deemed insufficient. To address risks associated with increased use of personal data, regulators and law makers in the AP region have introduced various laws and regulations on data privacy, data protection, and cybersecurity. The recent regulatory developments in operational resilience have also extended the regulatory scrutiny on the FS firm to outsourcing contractors, third-party vendors, and their subcontractors. Ensuring compliance with these regulations will be critical for FS firms adopting AI applications.

In some jurisdictions, any data requested from a customer must have a predetermined use and FS firms are not allowed to request and store data with an unconfirmed future intention to use in modelling. Therefore, adding data fields to on-boarding systems, without clearly identified use cases, can be challenging. In such cases, it is important to have a long term data strategy that is informed by relevant regulations.

What firms can do to align with the privacy and data security principles

1) Design and implement measures that ensure compliance with local data privacy laws and regulations throughout the life cycle of AI applications.
2) Incorporate data protection into the design of AI applications as well as the ongoing monitoring processes.
3) Develop a long-term data strategy that is in line with both the business needs and relevant data protection laws and regulations.

Adopting a trustworthy AI framework

While AI applications can offer numerous benefits for FS firms, poor management of risks associated with these applications could potentially bring unintentional consequences that may undermine the trust between a firm and its stakeholders and defeat the purpose of implementing AI applications in the first place.

As outlined in this report, FS firms considering the adoption of AI applications should strengthen their technical capacity in AI to ensure the robustness of their AI applications and monitoring processes, as well as adopt a comprehensive trustworthy AI framework that addresses the principles of fairness, robustness, transparency, accountability, privacy and data security. We have also observed that AP regulators are converging towards these principles in their guidance on the use of AI in financial services.

The *Deloitte Trustworthy AI Framework* provides FS firms in the region with a framework to implement a systemic and comprehensive solution to mitigate legal and regulatory risks, while meeting evolving customer needs. In establishing their AI frameworks, FS firms should:

1. Set up a comprehensive governance framework, and corresponding policies and procedures to ensure accountability of AI applications.
2. Define a vision and a long-term AI strategy, capture firm-wide AI use cases, and assess their impact and feasibility, through impact assessments and gap analysis.
3. Develop the right AI solution and align on the above-mentioned AI principles through white-boxing and bias/robustness assessments.
4. Deploy the AI applications into the system landscape and secure IT safety.
5. Assess and validate if data pipelines and algorithms work as expected through continuous monitoring and evaluation.

The call for ethical and trustworthy AI goes beyond consumer and regulatory expectations. As noted above, the *EU Ethics Guidelines for Trustworthy AI* and *Australia's Ethical AI Framework* both explicitly call for protection of human autonomy and oversight, as well as supporting social and environmental well-being when using AI. To ensure that the use of AI serves society and is not contrary to human welfare, FS firms should consider taking the following measures:

1. Verify that AI applications are compliant with laws and regulations.
2. Set ethical AI standards that are in line with the firm's values and culture.
3. Define specific concepts, principles and commitments based on the firm's ethical AI standards.
4. Incorporate the concepts, principles and commitments into policy and procedures of the firm's operations and the AI model governance framework to make justifiable decisions.
5. Educate all staff members on the firm's ethical AI standards and provide all staff members with an avenue to provide input into what ethical considerations must be considered.

While it is a major undertaking for FS firms to set an ethical framework and operationalise it across functions, it is important as FS firms are key members of society. They have a social responsibility to ensure the ethical and trustworthy use of AI as it becomes more and more pervasive in our daily lives. Collectively, such a human-centric use of AI and big data can help shape an inclusive, safe, and prosperous future for all of us.

Contacts

Seiji Kamiya
ACRS Executive Sponsor
RA AP Regulatory and Legal Support Leader
seiji.kamiya@tohmatsu.co.jp
+81 8034 69 5275

Mike Ritchie
Australia Co-lead
Partner, Risk Advisory
Financial Services Industry Lead, Asia Pacific
miritchie@deloitte.com.au
+61 2 9322 3219

Nai Seng Wong
Southeast Asia Co-lead
Partner, Risk Advisory
Regulatory Strategy Leader, SEA
nawong@deloitte.com
+65 6800 2025

Shinya Kobayashi
Japan Co-lead
Managing Director, Risk Advisory
Financial Industry Risk & Regulation
shinya.kobayashi@tohmatsu.co.jp
+81 807 196 8915

Jaramie Nejal
Operations Lead
Director, Risk Advisory
Financial Industry Risk & Regulation
jnejal@deloitte.com.au
+61 419 566 798

Authors

Ningxin Su
Manager
Hong Kong SAR
nsu@deloitte.com.hk

Lisa Kahlen
Manager
Australia
likahlen@deloitte.com.au

Suleigh Huang
Senior Analyst
Australia
sulhuang@deloitte.com.au

Winifred Lu
Senior Consultant
Hong Kong SAR
winlu@deloitte.com.hk

Acknowledgments

Australia

Sean Moore
Partner

Elea Wurth
Partner

Thomas Kohlborn
Director

Richard Kelly
Senior Manager

Maryam Fanaeepour
Specialist Manager

Darren Lawton
Specialist Manager

China

Roman Fan
Partner

Luke Lu
Senior Manager

Daniel Ma
Senior Data Scientist

Xiaoyu Li
Senior Data Engineer

Japan

Shiro Katsufuji
Managing Director

Southeast Asia

Dishell Gokaldas
Partner
Singapore

Mark Woodley
Partner
Indonesia

Thao Nguyen
Director
Vietnam

Jiejie Zhang
Senior Manager
Singapore

Thai Doan
Manager
Vietnam

Jennifer Martiniak
Associate
Singapore

Endnotes

1. NVIDIA, *State of AI in Financial Services - 2022 Trends, 2022*, https://www.nvidia.com/content/dam/en-zz/Solutions/industries/finance/ai-financial-services-report-2022/fsi-survey-report-2022-web-1.pdf
2. Monetary Authority of Singapore, *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector,* November 2018, https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf
3. Monetary Authority of Singapore, *Implementation of Fairness Principles in Financial Institutions' Use of Artificial Intelligence / Machine Learning*, June 2022, https://www.mas.gov.sg/-/media/MAS-Media-Library/publications/monographs-or-information-paper/IMD/2022/Info-Paper-on-Implementation-of-Fairness-Principles-in-FIs-Use-of-AIML-Final.pdf
4. Australian Government Department of Industry, Science and Resources, *Australia's Artificial Intelligence Ethics Framework,* November 2019, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework
5. China Financial Standardization Technical Committee, *Evaluation specification of artificial intelligence algorithm in financial industry standard officially released,* June 2021, https://www.cfstc.org/en/2932554/2980201/index.html
6. European Commission, *Ethics Guidelines for Trustworthy AI,* April 2019, https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html
7. Australian Government Department of Industry, Science and Resources, *Australia's Artificial Intelligence Ethics Framework,* November 2019, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework
8. MIT Technology Review, *'Trustworthy AI' is a framework to help manage unique risk,* March 2020, https://www.technologyreview.com/2020/03/25/950291/trustworthy-ai-is-a-framework-to-help-manage-unique-risk/
9. Hong Kong Monetary Authority, *Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions,* November 2019, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf
10. Australian Government Department of Industry, Science and Resources, *Australia's AI Ethics Principles,* November 2019, https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles
11. Monetary Authority of Singapore, *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector,* November 2018, https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf
12. The OECD AI Policy Observatory, *Transparency and explainability (Principle 1.3),* May 2019, https://oecd.ai/en/dashboards/ai-principles/P7
13. European Commission, *Proposal for A Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,* April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
14. Monetary Authority of Singapore, FEAT Principle, Principle 1: *"Individuals or groups of individuals are not systematically disadvantaged through AIDA-driven decisions unless these decisions can be justified".*
15. Hong Kong Monetary Authority, Consumer Protection in respect of Use of Data Analytics and Artificial Intelligence by Authorized Institutions, Principle (c) on fairness: *"customers' financial capabilities, situation and needs, including their level of digital literacy, are taken into account."*
16. Monetary Authority of Singapore, FEAT Principle, Principle 3: *"Data and models used for AIDA-driven decisions are regularly reviewed and validated for accuracy and relevance, and to minimize unintentional bias."*
17. Monetary Authority of Singapore, *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector,* November 2018, https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf
18. Hong Kong Monetary Authority, *High-level Principles on Artificial Intelligence,* November 2019, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf

The Deloitte Centre for Regulatory Strategy is a source of critical insights and advice, designed to assist the world's largest financial institutions manage the strategic and aggregate impact of regional and international regulatory policy. With regional hubs in the Americas, Asia Pacific and EMEA, the Centre combines the strength of Deloitte's network of experienced risk, regulatory, and industry professionals — including a deep roster of former regulators, industry specialists, and business advisers — with a rich understanding of the impact of regulations on business models and strategy.

Deloitte.

Designed by CoRe Creative Services. RITM1170527

This is printed on environmentally friendly paper