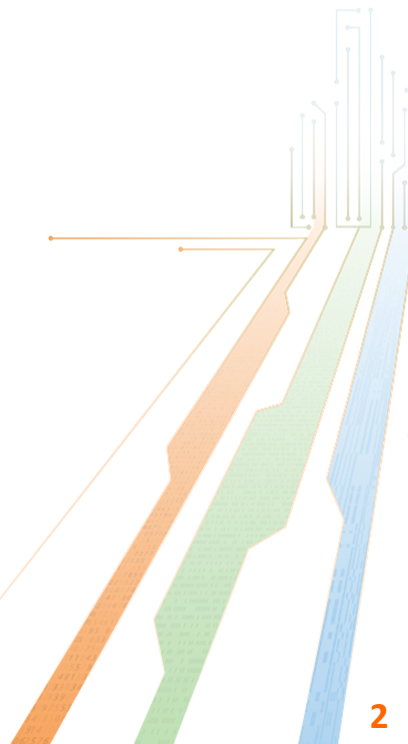
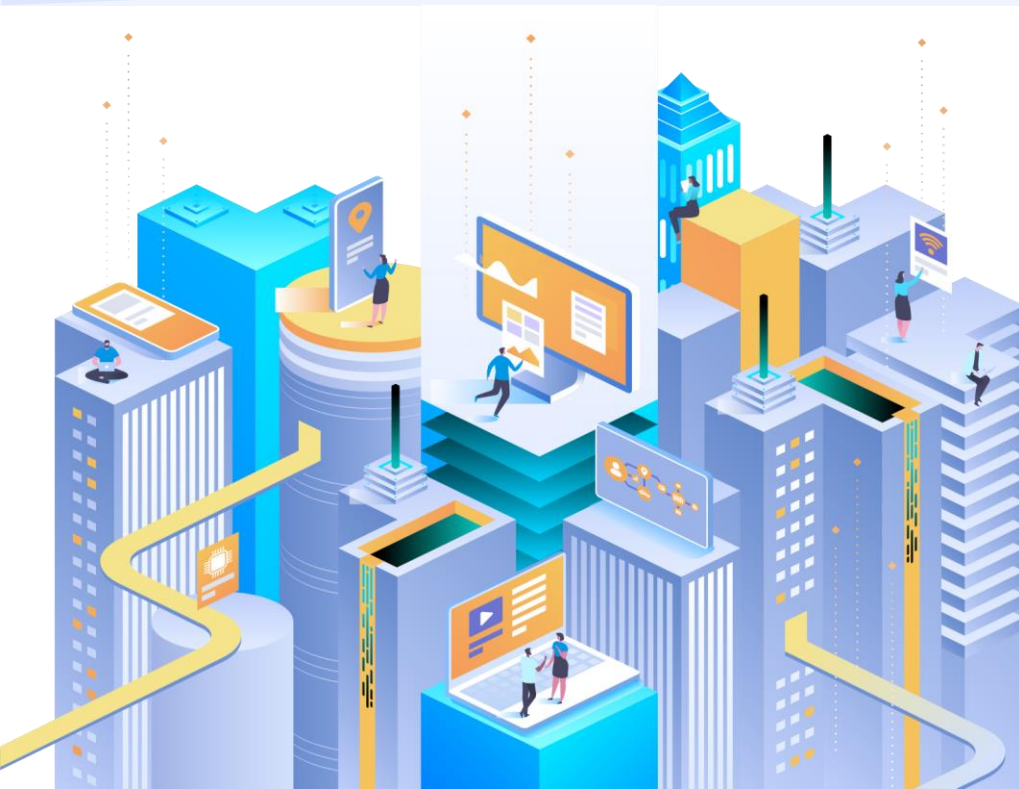


- 1 Challenges faced by financial services firms**
- 2 Risks arising from the use of AI**
- 3 Overview of "Ethical Development and Use of Artificial Intelligence" (2021)**
- 4 Overview of "Artificial Intelligence: Model Personal Data Protection Framework" (2024)**

1 Challenges faced by financial services firms

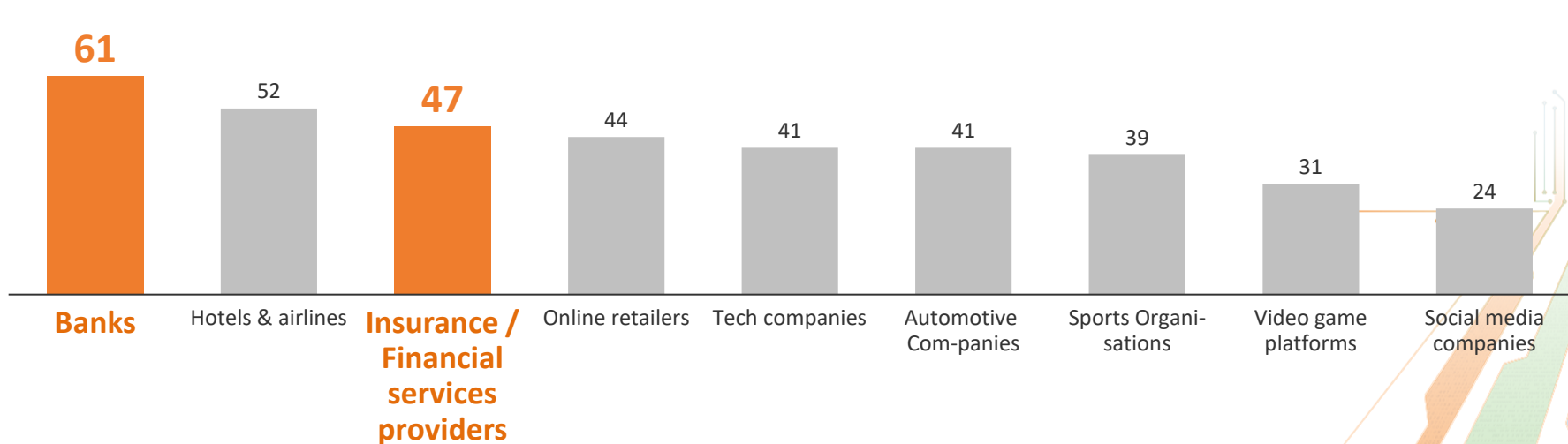


Good record

Finance-related organisations have enjoyed trust from customers

Which sectors do customers trust most with their personal data?

%, 2023, 18 markets across the world



Finance-related organisations ranked 1st and 3rd among industries

Source: [YouGov](#) (2023)

Challenge

Financial firms are prime targets for cyber criminals

Financial sector's exposure to cyber threats



Proportion of reported cyber incidents affecting the financial sector in the past 2 decades globally



Advanced economies

More exposed than firms in emerging market and developing economies

Source: IMF (2024)

Fund and wealth management activities are exposed to heightened risks



High-net-worth clients

Detailed records

- Income
- Tax information
- Investment strategies
- Details of family members

High potential value for cybercriminals

- Identity theft



Perceived ability to pay

Financial power

- Cybercriminals think financial firms will pay for ransom given their resources

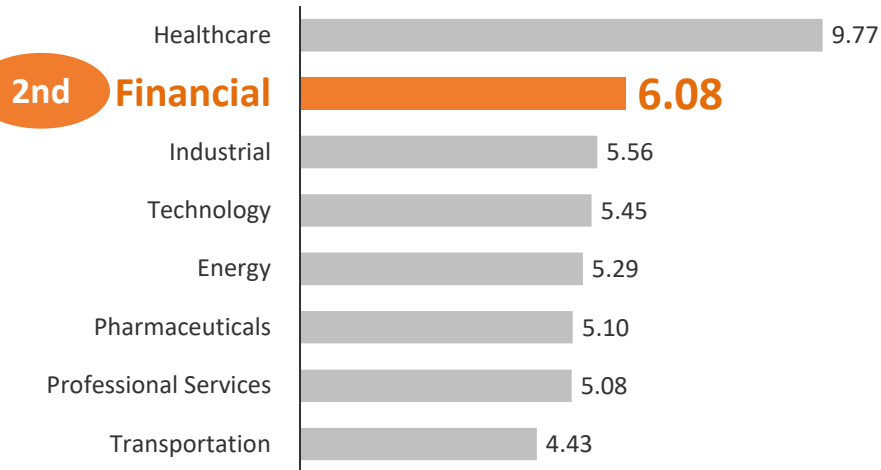
Cost

The cost of data breaches could run high

The cost of a data breach for the financial industry is among the highest

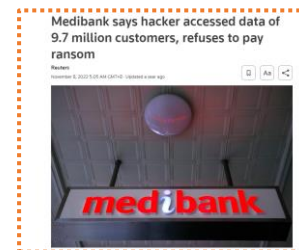
Cost of a data breach

USD millions, 2024, by industry



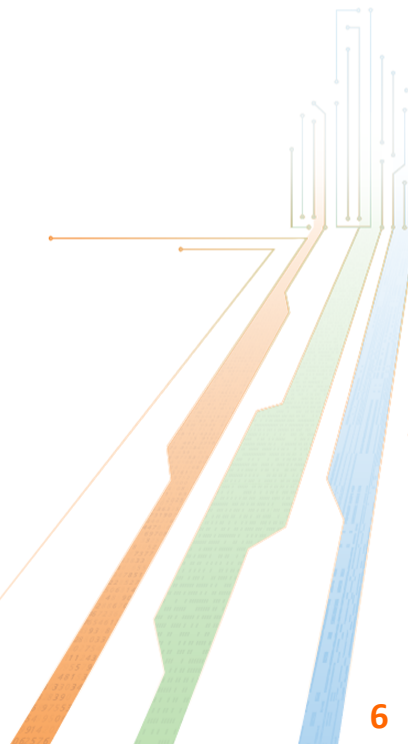
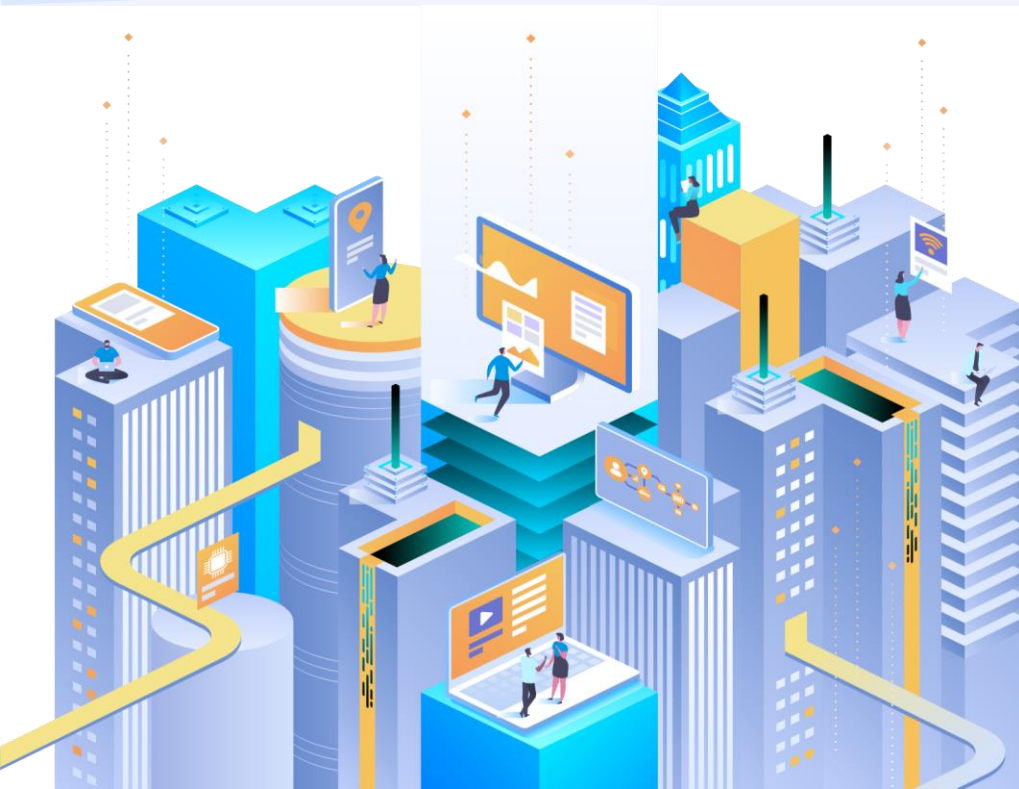
Source: [IBM](#)

Regulators have filed civil lawsuits against rule-breakers



- Hackers used the **credential stolen** from an account with preferential access to the internal system
- Health data of over **9 million customers released on the dark web**
- Australian Information Commissioner filed civil penalty proceedings against Medibank in June 2024, with maximum **penalty of AUD2.22 million for each contravention**

2 Risks arising from the use of AI



Risks

AI has further complicated the picture, with new risks arising

1



Privacy risks



Excessive data collection



Misuse of data



Data security



Identity re-identification



Data accuracy

2



Ethical risks



Interpretation of decisions



Harmful content



Bias and inaccuracies



Hallucination



Copyright issues

Data at Stake

A lot of personal data could be involved in wealth management

Initial contact

Initial Consultation

Customer segmentation

Regulatory checks

Name screening

Enhanced Due Diligence

Data analysis and goal setting

Data analysis to establish tailored financial goals

Implementation & Monitoring

Execute investment strategies

Review and change strategies as circumstances change

Monitor and report on the plan

Personal information

- Names
- Contact details (Addresses, phone numbers, email addresses)
- Health
- Lifestyle information (politically exposed?)

Family information

- Names
- Ages

Financial Information

- Income & employment details
- Assets and liability
- Transaction history

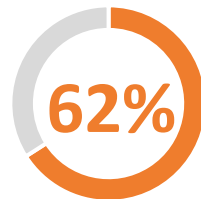
Public's reaction

The public is concerned about organisation's use of data in AI



Consumer's views towards business use of AI

Global consumers, 2023



Concerned about business use of AI



Use of AI by organisations has already eroded trust in them

Source: [Cisco](#)







Organisation's awareness

Organisations see genAI as posing higher privacy risks

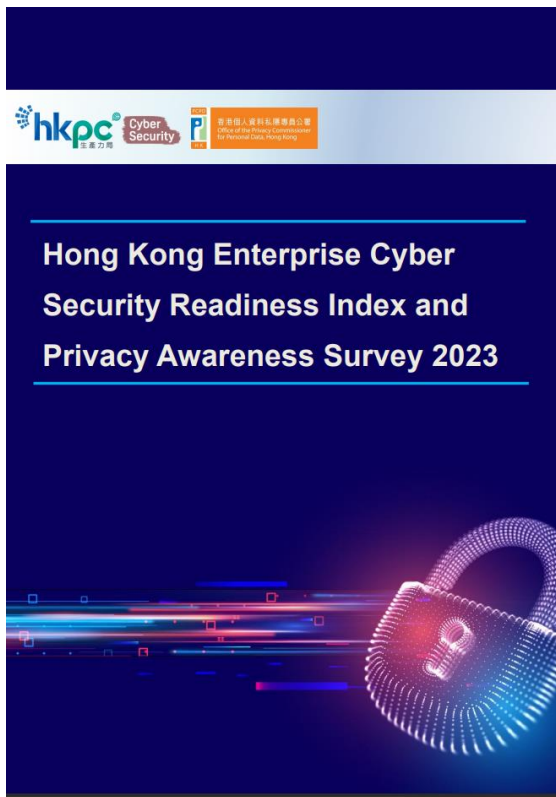
Privacy risks among emerging technologies

Hong Kong enterprises, 2023

Highest
Risk
Level

-  **Generative AI**
-  Cookies and other online trackers
-  Cloud computing
-  Internet of Things
-  Blockchain related technology
-  Data analytics and work process automation

Source: PCPD & HKPC



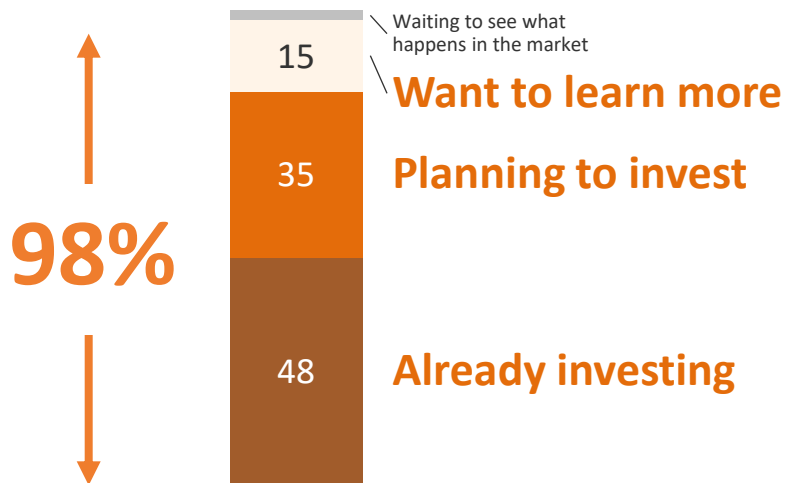
Dare not use

Yet, it seems the use of AI is a matter of when, but not if

Most wealth and asset managers are investing or planning to investing AI

Investment in genAI

Wealth and asset managers, 2023

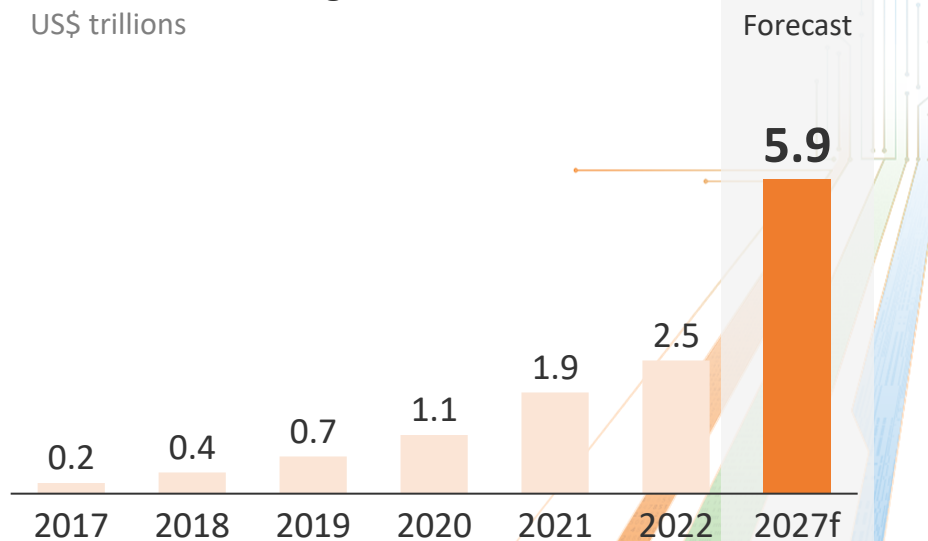


Source: EY

Assets managed by robo-advisors will double in a few years' time

Assets under management of robo-advisors

US\$ trillions

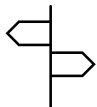


Source: PwC

Benefits

Good use of AI could unleash lots of potential

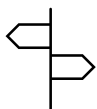
Potential Benefits



Customer identification



Enhanced due diligence



Streamlined workload



Better investment strategies

Source: [Financial Times](#); [Forbes](#); [EY](#)

Technology

JPMorgan Gives Staff AI-Powered 'Research Analyst' Chatbot

- CEO Jamie Dimon has likened AI tech to steam engine, internet
- Asset and wealth management employees given access to the tool



Source: [Bloomberg](#)

Morgan Stanley Wealth Management Announces Latest Game-Changing Addition to Suite of GenAI Tools

Jun 26, 2024

AI @ Morgan Stanley Debrief acts as notetaker, summarizer and first draft communication composer for client meetings, greatly enhancing efficiency and enabling scale for Advisors and their practices

Source: [Morgan Stanley](#)

Best of both worlds

Is it possible to enjoy benefits of AI while ensuring privacy protection?

Privacy risks need to be carefully managed



Opportunities from AI need to be grabbed

Source: AI-generated image from Microsoft Copilot

4

Overview of "Ethical Development and Use of Artificial Intelligence" (2021)



Foundation

The below values and principles ensure ethical use of AI



3 Data Stewardship Values



1. Being Respectful



2. Being Beneficial



3. Being Fair



7 Ethical Principles for AI



1. Accountability



3. Transparency & Interpretability



5. Fairness



2. Human Oversight



4. Data Privacy

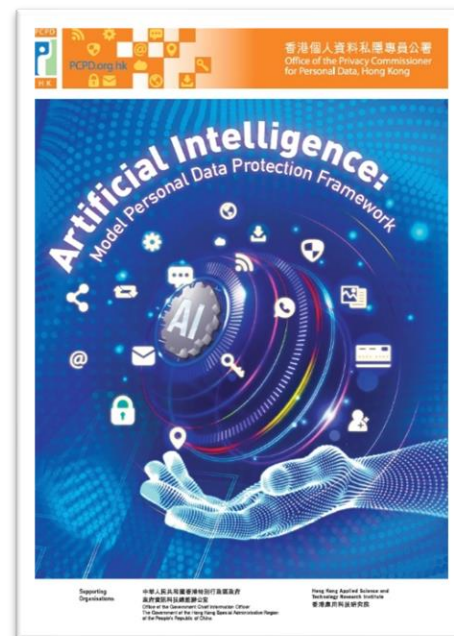


6. Beneficial AI



7. Reliability, Robustness & Security

5 Overview of "Artificial Intelligence: Model Personal Data Protection Framework" (2024)



Foundation models

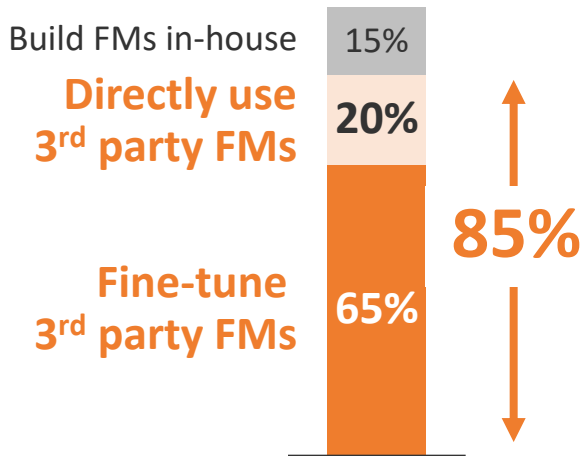
Enterprises may use third-party FMs more than to develop in-house models

Most firms won't develop FMs in-house

Enterprises will tilt towards customising 3rd party FMs for cost and speed reasons

Intended FM model use

US, Telecommunications sector, %

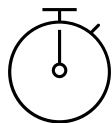


In-house development



Cost

- Building one model can cost US\$50-90 million



Time

- 3 – 6 months for developing one model

Third-party FMs

- Fine-tuned FMs
- Off-the-shelf FMs

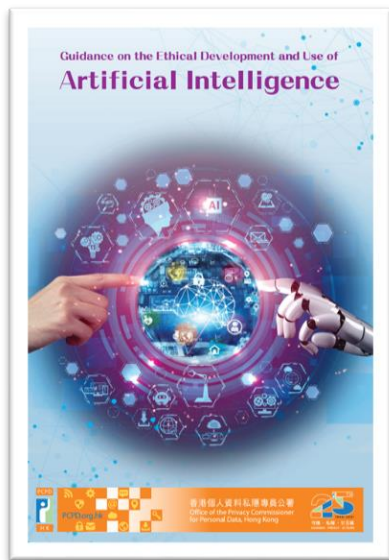
- Fast even with data training
- Up to 70% reduction in time to value

Source: [AWS](#)

Source: [BCG](#); [IBM](#)

International standards

The Framework aligns with internationally recognised values and principles



3 Data Stewardship Values



1. Being respectful



2. Being beneficial



3. Being fair

7 Ethical Principles for AI

1. Accountability

4. Data Privacy

2. Human oversight

5. Fairness

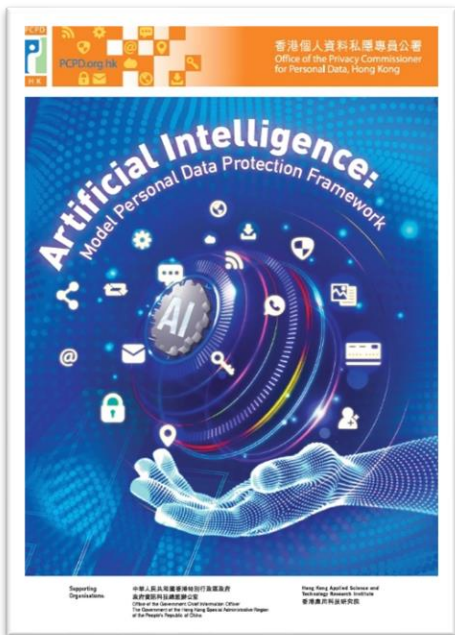
3. Transparency & interpretability

6. Beneficial AI

7. Reliability, robustness & security

Model Personal Data Protection Framework

Artificial Intelligence: Model Personal Data Protection Framework



Feature



A set of recommendations on the best practices for organisations procuring, implementing and using any type of AI systems, including generative AI, that involve the use of personal data

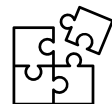
Benefits



Assist organisations in complying with the requirements of the Personal Data (Privacy) Ordinance



Nurture the healthy development of AI in Hong Kong

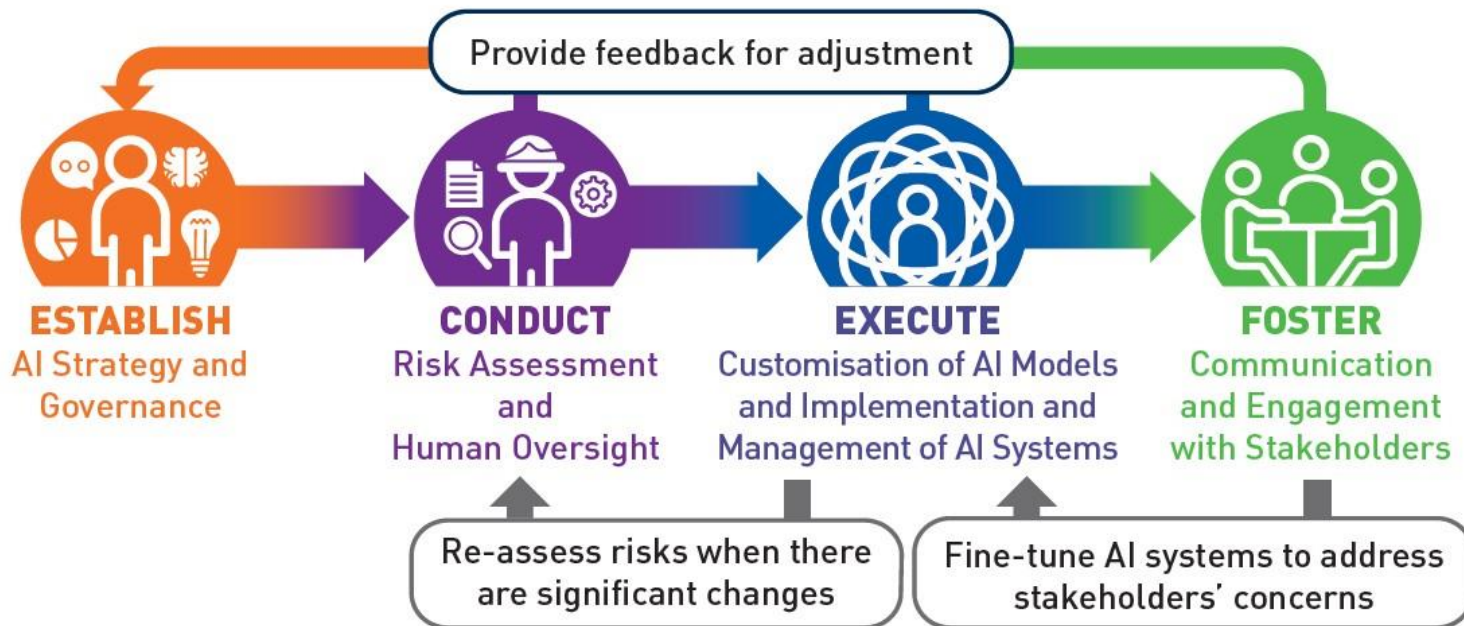


Facilitate Hong Kong's development into an innovation & technology hub



Propel the expansion of the digital economy not only in HK but also GBA

Artificial Intelligence: Model Personal Data Protection Framework



Establish

AI Strategy and Governance



1

AI Strategy

3

Governance
Considerations for
Procuring AI
Solutions

2

Governance
Structure

4

Training and
Awareness Raising

AI Strategy

An AI strategy shows management's commitment



1.1 AI Strategy

1.2 Governance Considerations

1.3 Governance Structure

1.4 Training

AI Strategy

Functions



Demonstrate the commitment of top management to the ethical and responsible procurement, implementation and use of AI



Provide directions on the purposes for which AI solutions may be procured, and how AI systems should be implemented and used

Elements that may be included



Setting out **ethical principles**



Establishing **specific internal policies and procedures**



Determining **unacceptable uses** of the AI systems



Regularly **communicating the AI strategy, policies and procedures**



Establishing an **AI inventory**



Considering **emerging laws and regulations** that may be applicable

AI procurement steps

AI solution procurement generally involves 7 steps



ESTABLISH
AI Strategy and
Governance

1.1 AI Strategy

1.2
Governance
Considerations

1.3
Governance
Structure

1.4 Training



1. Sourcing AI solutions



**2. Picking the
appropriate AI solution**



**3. Collecting and
preparing data**



**4. Customising AI model
for particular purpose**



**5. Testing, evaluating and
validating AI model**



**6. Testing and auditing system
and components for
security and privacy risks**



**7. Integrating AI solution
into organisation's system**

Governance considerations

An organisation intending to invest in AI solutions may consider



ESTABLISH
AI Strategy and
Governance

1.1 AI Strategy

1.2
Governance
Considerations

1.3
Governance
Structure

1.4 Training



Purpose(s) of using AI



**Privacy and security
obligations and ethical
requirements**



**International technical
and governance
standards**



**Criteria and procedures
for reviewing AI
solutions**



**Data processor
agreements**



**Policy on handling output
generated by the AI
system**



**Plan for continuously
scrutinising changing
landscape**



**Plan for monitoring,
managing and
maintaining AI solution**



Evaluation of AI supplier

Governance Structure

An internal governance structure with sufficient resources, expertise and authority should be established



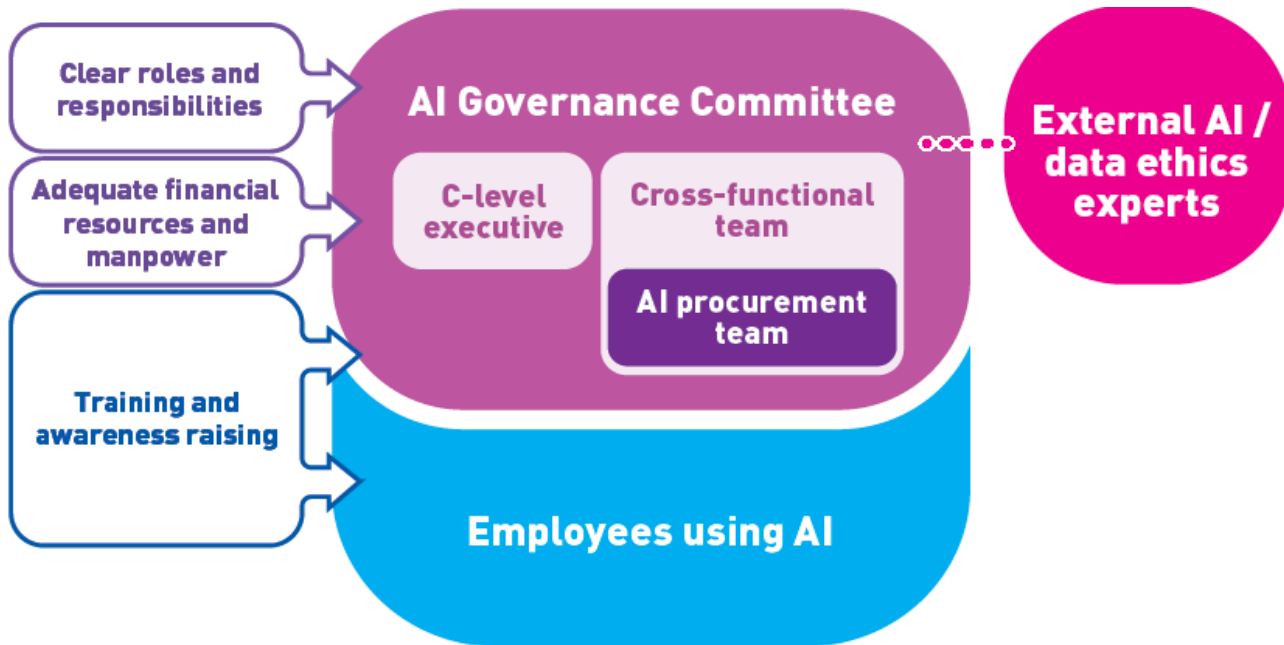
ESTABLISH
AI Strategy and
Governance

1.1 AI Strategy

1.2
Governance
Considerations

1.3
Governance
Structure

1.4 Training



Training and Awareness Raising

Different personnel should receive training tailored for them



1.1 AI Strategy

1.2
Governance
Considerations

1.3
Governance
Structure

1.4 Training



Recommended Personnel



**System analysts/architects
/ data scientists**



AI system users



**Legal and compliance
professionals**



Procurement staff



Human reviewers



**All staff performing
work relating to AI
system**



Training Topics

- Compliance with data protection laws, regulations and internal policies; cybersecurity risks
- Compliance with data protection laws, regulations and internal policies; cybersecurity risks; general AI technology
- General AI technology and governance
- General AI technology and governance
- Detection and rectification of any unjust bias, unlawful discrimination and errors / inaccuracies in the decisions made by AI systems or presented in the content
- Benefits, risks, functions and limitations of the AI system(s) used by the organisation

Conduct

Risk assessment and human oversight



Process of Risk Assessment

1

Conduct risk assessment by a cross-functional team

2

Identify and evaluate the risks of the AI system

3

Adopt risk management measures

Risk-based approach

The level of human oversight should correspond with the risks identified



2.1 Risk
Factors

2.2 Human
Oversight

2.3 Risk
Mitigation
Trade-offs



Examples

The below use cases may incur higher risks



CONDUCT
Risk Assessment
and
Human Oversight

2.1 Risk
Factors

2.2 Human
Oversight

2.3 Risk
Mitigation
Trade-offs



Real-time identification of individuals using biometric data



Evaluation of individuals' eligibility for social welfare or public services



Assessment of job applicants, evaluation of job performance or termination of employment contracts



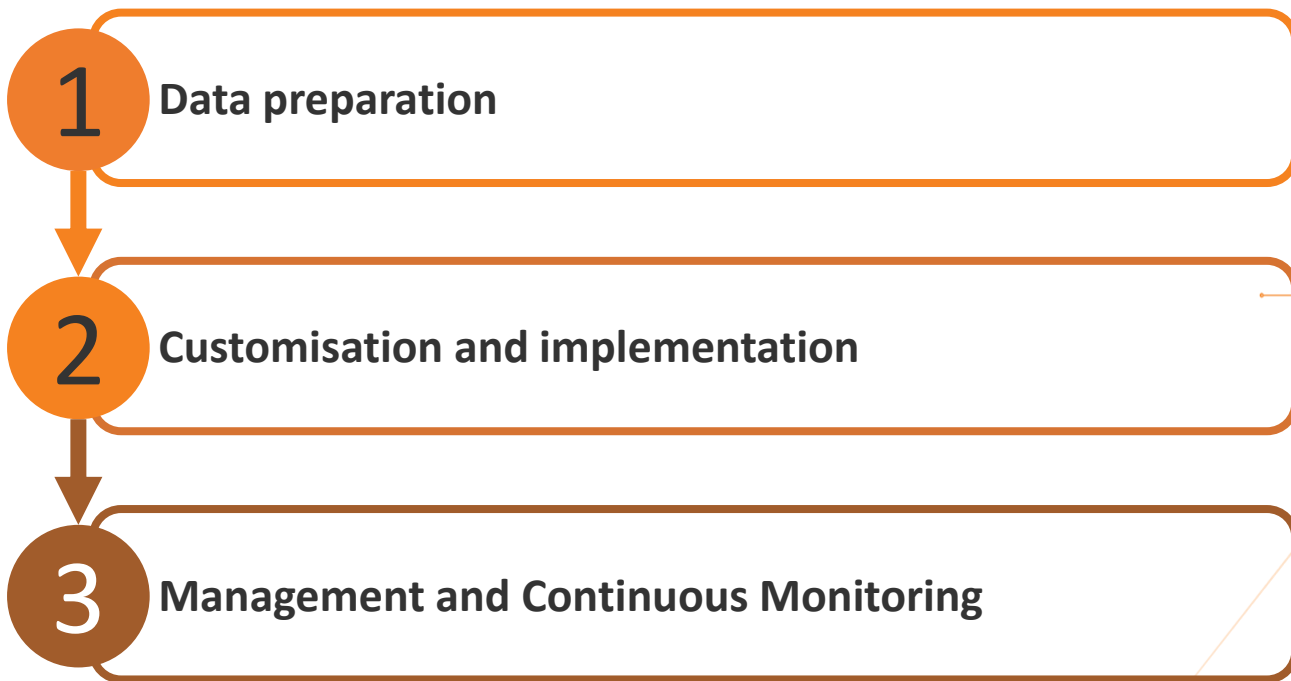
Evaluation of the creditworthiness of individuals for making automated financial decisions



AI-assisted medical imaging analytics or therapies

Execute

Customisation of AI Models and implementation and management of AI systems



Data Preparation

Compliance, data minimization, quality management, data handling

Selected Recommendations



Ensure compliance with privacy law



Minimise the amount of personal data involved



Manage data quality



Document data handling

Example

- A fashion retail platform is **purchasing a third-party developed AI chatbot** that it will customise to provide **fashion recommendations** to its customers
- The company may find it **necessary** to use the **past purchases** and **browsing histories** of **different segments** of its customer groups to fine-tune the chatbot
- However, the use of **personal data**, such as customers' names, contact details and certain demographic characteristics, would **not be necessary**



3.1 Data Preparation

3.2 Customisation Implementation

3.3 Management & Monitoring

AI Incident Response Plan

All six steps in a glance



3.1 Data
Preparation

3.2
Customisation
Implementation

3.3
Management &
Monitoring

1



Defining an AI
Incident

3



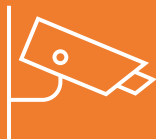
Reporting an
AI Incident

5



Investigating an
AI Incident

2



Monitoring for
AI Incidents

4



Containing an
AI Incident

6



Recovering from
an AI Incident

Foster

Communication and Engagement with Stakeholders



1

Information Provision

2

Data Subject Rights and Feedback

3

Explainable AI

4


Language and Manner

Contact Us

 **Hotline** 2827 2827  **Fax** 2877 7026

 **Website** www.pcpd.org.hk

 **Email** communications@pcpd.org.hk

 **Address** Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen' s Road East, Wanchai, Hong Kong

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

Follow us



Disclaimer

- The information provided in this PowerPoint for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (Cap 486) (“**PDPO**”).
- For a complete and definitive statement of law, direct reference should be made to the PDPO itself.
- The Office of the Privacy Commissioner for Personal Data makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this PowerPoint.
- The contents provided will not affect the exercise of the functions and powers conferred to the Commissioner under the PDPO.