



PCPD



HK

香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

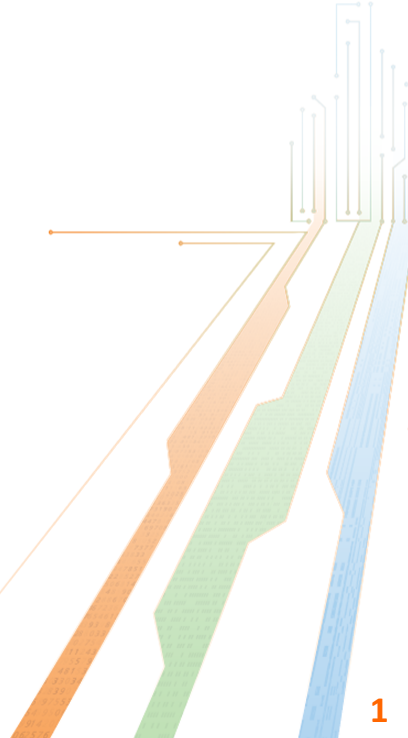
## ***Artificial Intelligence: Model Personal Data Protection Framework***

**Hong Kong General Chamber of  
Commerce**

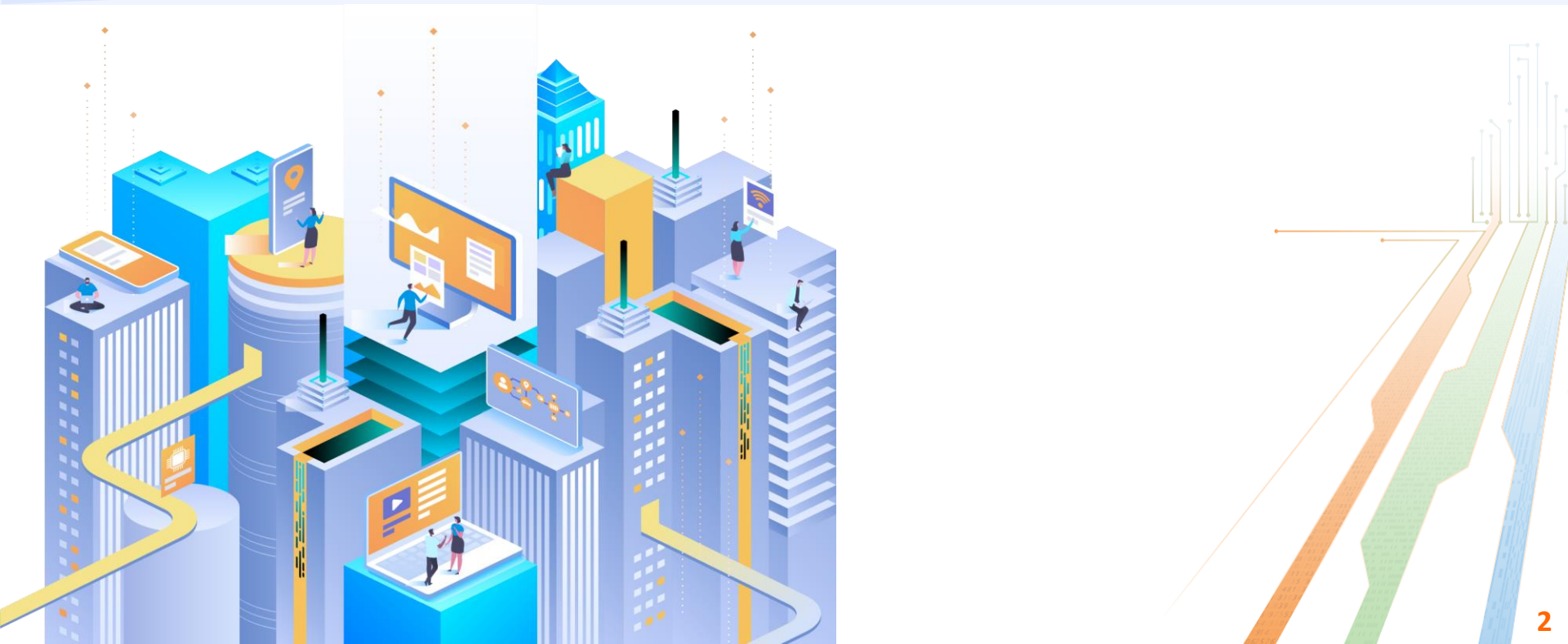
**20 September 2024**

**Joyce Liu, Ag. Senior Legal Counsel &  
Head of Global Affairs and Research, PCPD**

- 1 Impact and risks of AI
- 2 Overview of "Artificial Intelligence: Model Personal Data Protection Framework" (2024)
- 3 Implementation



# 1 Impact and risks of AI



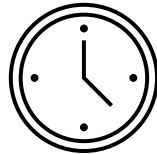
# Potential

AI characters could be very powerful

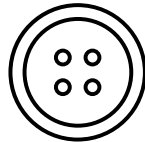
## Why AI characters can be more promising – and concerning



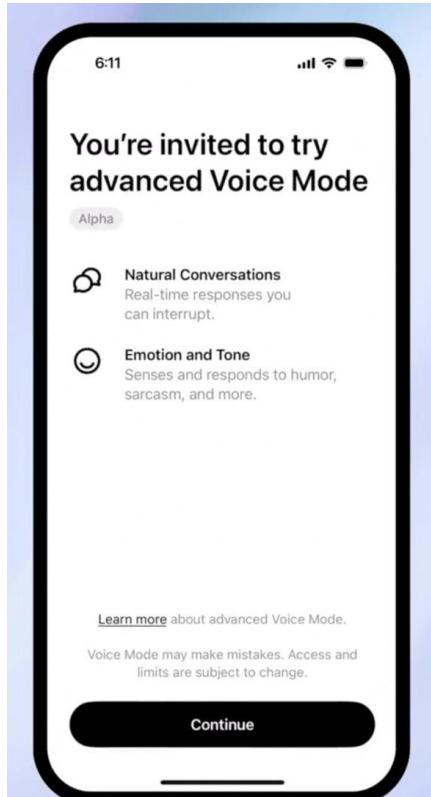
**Sophisticated understanding**



**24/7 availability**



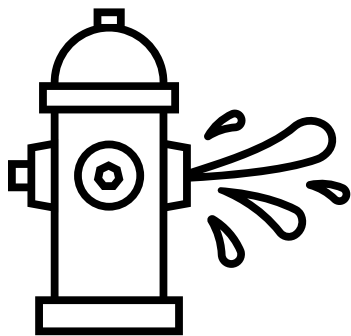
**Personalised experience**



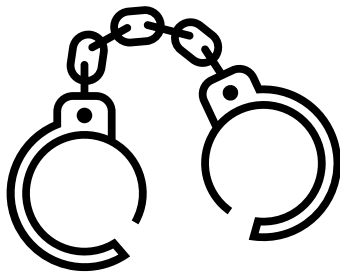
# Why care

AI impacts business very much

## How use of AI could impact businesses



**Data Breach**



**Regulatory requirements**



**Reputation**

# Security

Many employees insecurely use AI chatbots for work

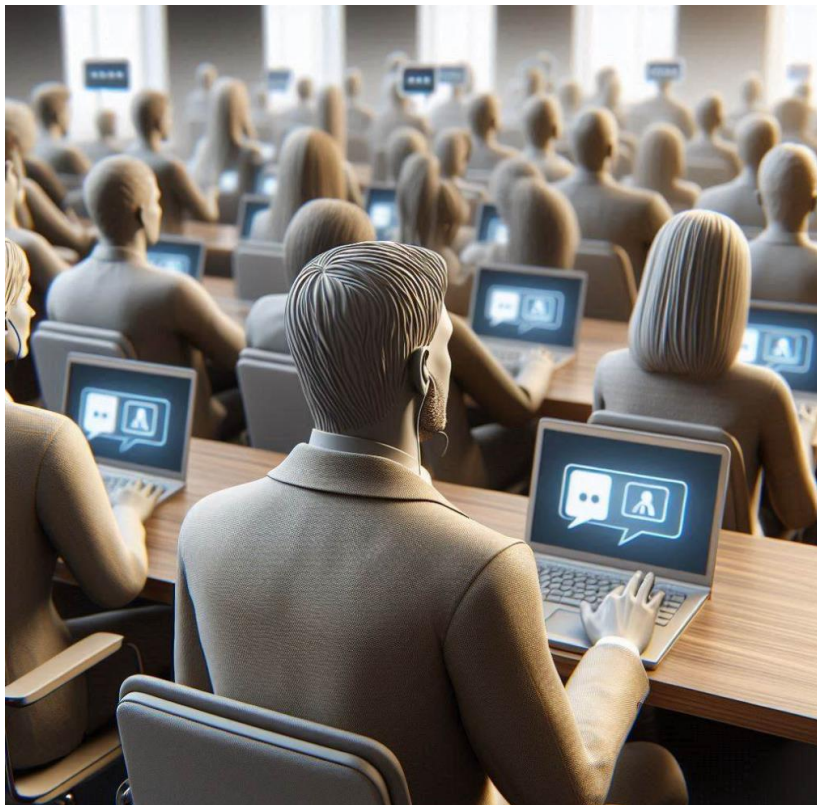


Image source: Microsoft Copilot Image Generator

## Prevalent insecure use of AI chatbots



**~75% of employees using ChatGPT use a private account**



**~28% data input into AI chatbots are sensitive**



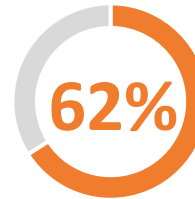
# Public's reaction

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

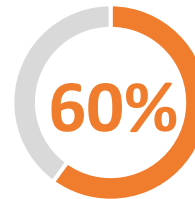


## Consumer's views towards business use of AI

Global consumers, 2023



Concerned about business use of AI



Use of AI by organisations has already eroded trust in them

# Risks

Different risks have arisen from AI

1



**Privacy risks**



**Excessive data collection**



**Misuse of data**



**Data security**



**Identity re-identification**



**Data accuracy**

2



**Ethical risks**



**Interpretation of decisions**



**Harmful content**



**Copyright issues**



**Bias and inaccuracies**



**Hallucination**



# Best of both worlds

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

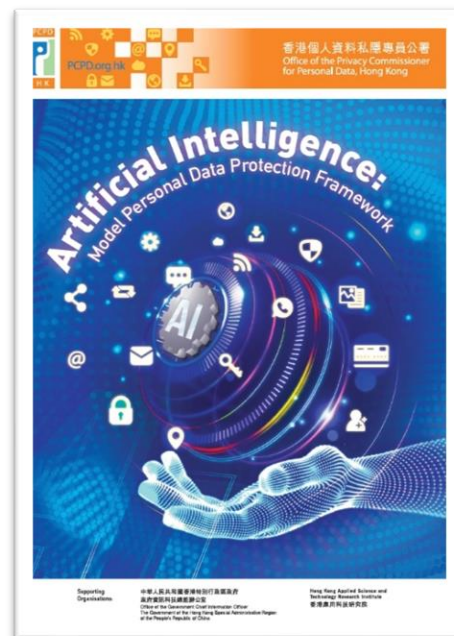
Privacy risks need to be carefully managed



Opportunities from AI need to be grabbed

2

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



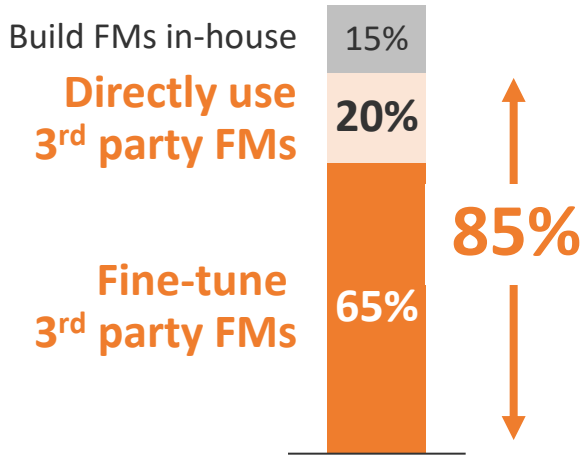
# Foundation models

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

Most firms won't develop FMs in-house

## Intended FM model use

US, Telecommunications sector, %



Source: [AWS](#)

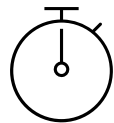
Enterprises will tilt towards customising 3<sup>rd</sup> party FMs for cost and speed reasons

## In-house development



Cost

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



Time

- 3 – 6 months for developing one model

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

## Third-party FMs

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

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

# 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

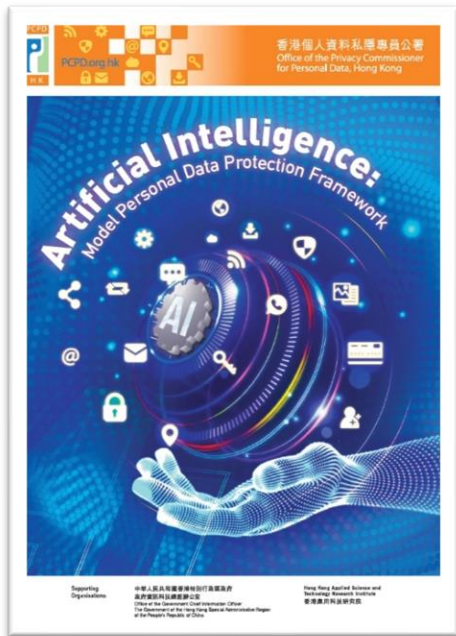
3. Transparency & interpretability

6. Beneficial AI

7. Reliability, robustness & security

Model Personal Data Protection Framework

# Artificial Intelligence: Model Personal Data Protection Framework



## Feature

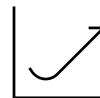


A set of recommendations on the best practices for organisations **procuring, implementing and using any type of AI systems**, including generative AI, that involve the use of personal data

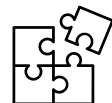
## Benefits



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



Nurture the healthy development of AI in Hong Kong



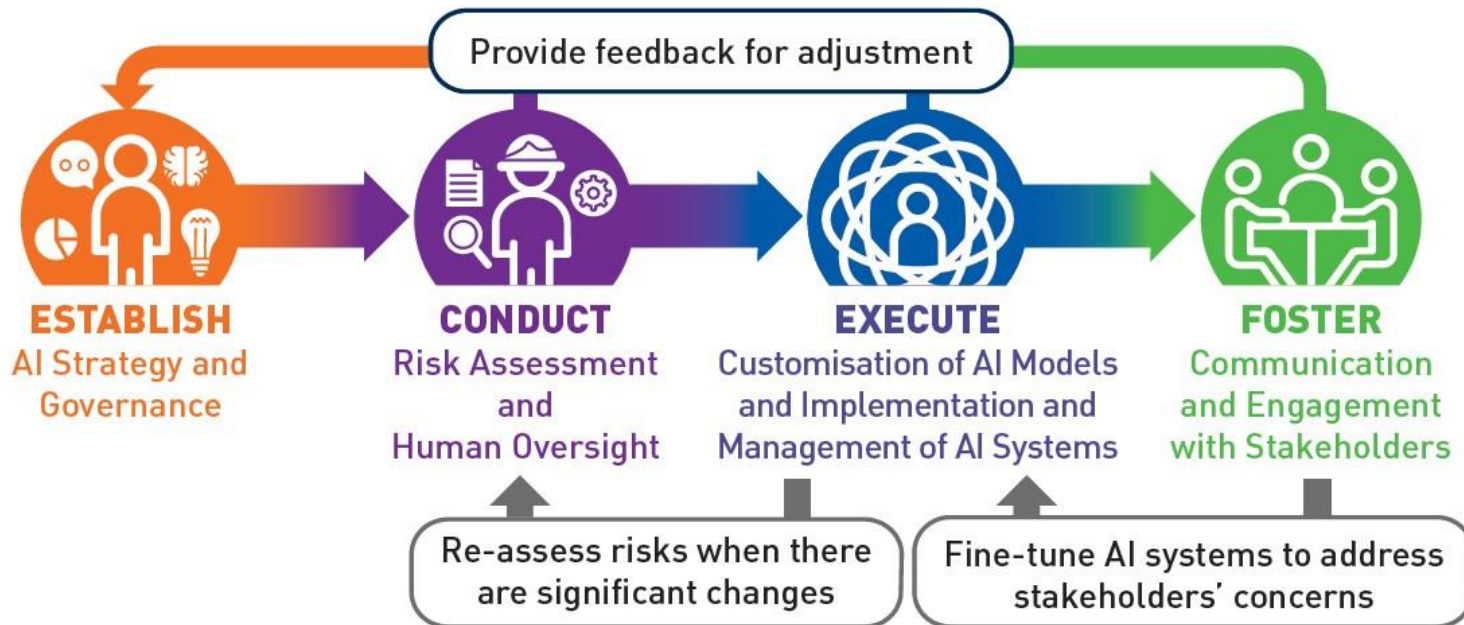
Facilitate Hong Kong's development into an innovation & technology hub



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



# Artificial Intelligence: Model Personal Data Protection Framework



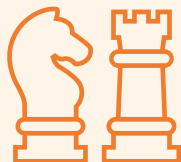


# Establish

## AI Strategy and Governance



1



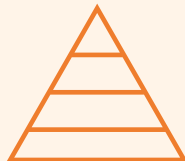
AI Strategy

3



Governance Considerations  
for Procuring AI Solutions

2



Governance  
Structure

4



Training and Awareness  
Raising

# AI Strategy

An AI strategy shows management's commitment



**ESTABLISH**  
AI Strategy and  
Governance

## 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**



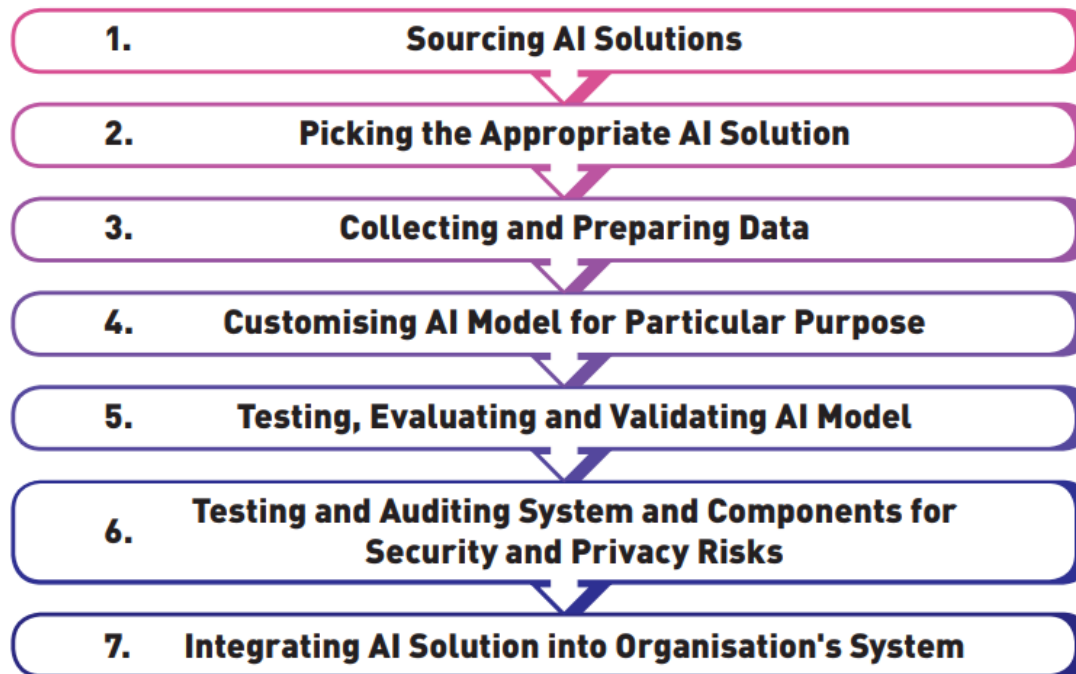
Establishing an **AI inventory**



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

# AI procurement steps

AI solution procurement involves 7 steps



# Governance considerations

An organisation intending to invest in AI solutions may consider



**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**



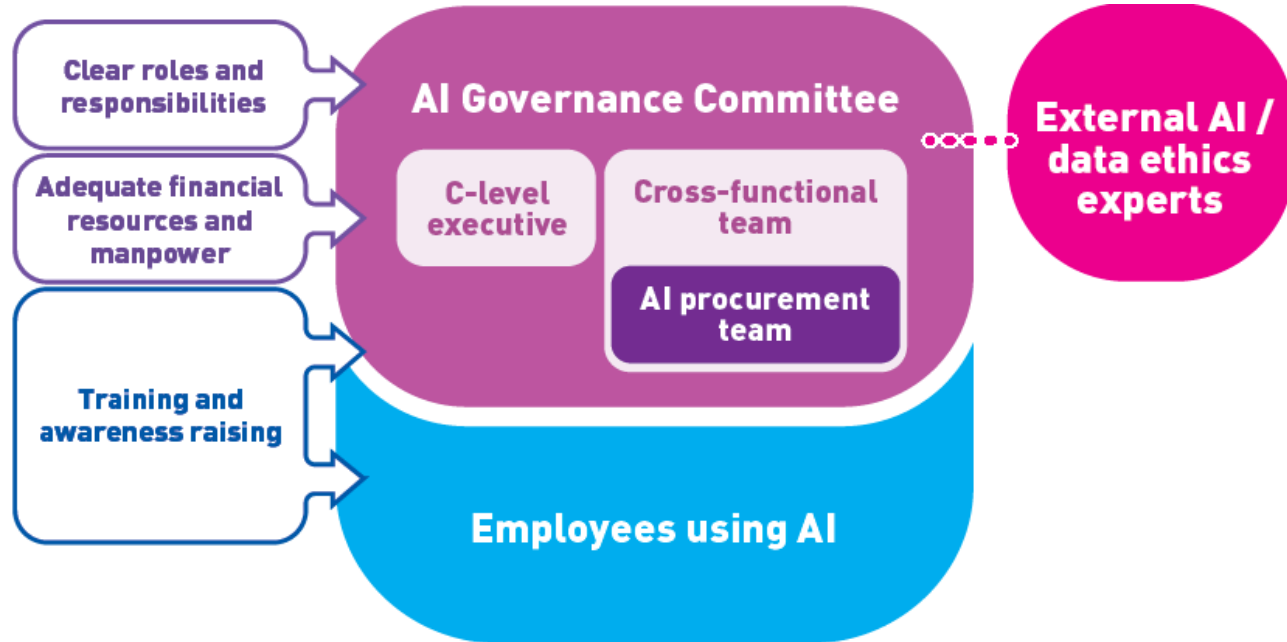
**Plan for monitoring, managing and maintaining AI solution**



**Evaluation of AI supplier**

# Governance Structure

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



# 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

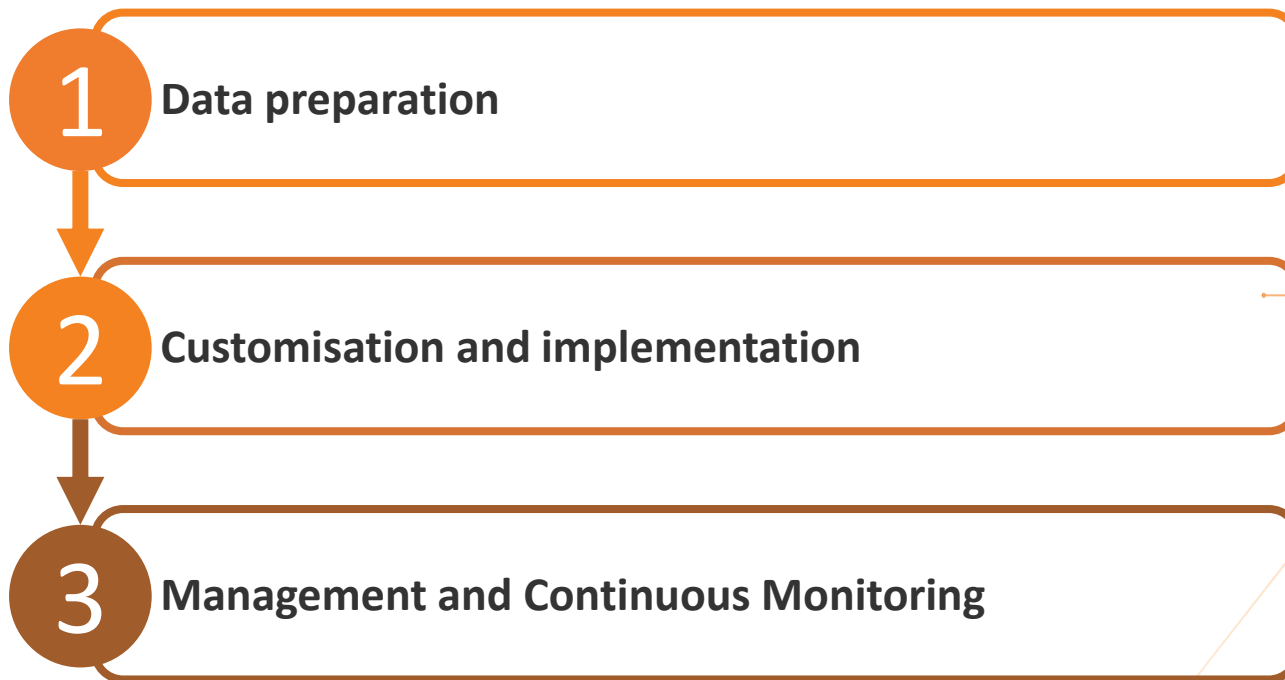


An AI system likely to **produce an output** that may have such **significant impacts** on individuals would generally be considered **high risk**.













# Execute

Customisation of AI Models and implementation and management of AI systems



# Data Preparation

Compliance, data minimization, quality management, data handling

Process	Selected Recommendations	
 <p><b>Data Preparation</b></p>	 <p>Ensure compliance with privacy law</p> <p>↓</p> <p>Minimise the amount of personal data involved</p>	 <p>Manage data quality</p>  <p>Document data handling</p>
 <p><b>Customisation and Implementation of AI</b></p>	<input checked="" type="checkbox"/> Conduct rigorous testing and validation of reliability, robustness and fairness	
 <p><b>Management and Continuous Monitoring of AI</b></p>	 <p>Maintain proper documentation</p>  <p><b>Establish an AI Incident Response Plan</b></p>	 <p>Conduct periodic audits</p>  <p>Consider incorporating review mechanisms as risk factors evolve</p>



# AI Incident Response Plan

All six steps in a glance



**The case of self-driving cars**

Image source: [Wikimedia Commons](#) (no changes made)

1

Defining an AI Incident

2

Monitoring for AI Incidents

3

Reporting an AI Incident

4

Containing an AI Incident

5

Investigating an AI Incident

6

Recovering from an AI Incident

# Foster

## Communication and Engagement with Stakeholders



1

**Information  
Provision**

3

**Explainable AI**

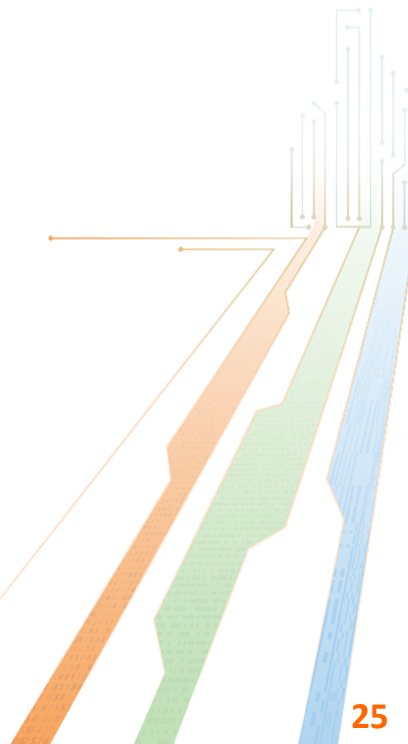
2

**Data Subject Rights  
and Feedback**

4

**Language and  
Manner**

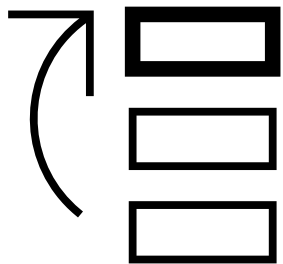
# 3 Implementation



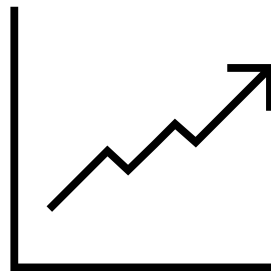


# Business-friendly

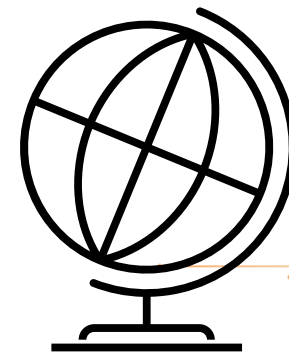
We've designed the Model Framework to be business-friendly



Best practices



Risk-based  
Approach



Alignment with  
international  
standards

# Questions

Businesses may ask why they should adopt the Framework

**1** How will this framework help my business build trust with customers?

**2** Can this framework help my business avoid regulatory pitfalls?

**3** My organisation is quite established, and we already have had our AI frameworks. Why should we still care about this Model Framework?

# PCPD's support

We're here to help



SME  
Hotline

## Seminar on "AI and Privacy Protection: Balancing Innovation and Safety"



**Ms Ada CHUNG Lai-ling**  
Privacy Commissioner  
for Personal Data



**Dr Arvin TANG**  
Director, Multimedia Systems and  
Analytics, Artificial Intelligence and  
Trust Technologies, ASTRI

30 July 2024 (Tuesday) | 3:00 pm - 4:15 pm

## Experience Sharing Session for Businesses on "AI and Personal Data Privacy"

30 Sep 2024 (Mon) | 3:00 pm - 4:15 pm



**Ms Amy LAM**  
Deputy Privacy Commissioner  
for Personal Data  
PCPD



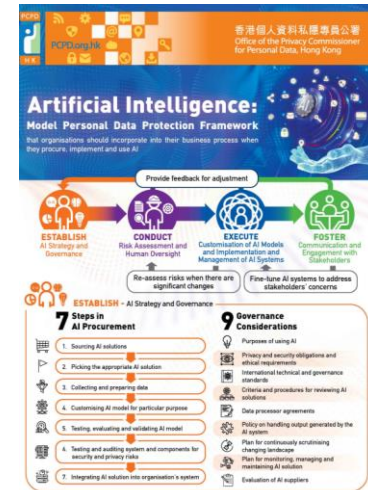
**Mr Aaron BLEASDALE**  
Managing Associate General Counsel  
and Head of Data Legal, Asia Pacific  
HSBC



Organiser:



Supporting  
Organisation:



2-page  
leaflet

Webinars

# Future

Together we could build a future with ethical and privacy-friendly AI



**Where our next generations benefit from AI's enormous powers**




**Because we act now to ensure the safety of AI by proactively managing its risks**

# Contact Us

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

 **Website** [www.pcpd.org.hk](http://www.pcpd.org.hk)

 **Email** [communications@pcpd.org.hk](mailto: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

