



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

Getting Ready for 2025: Action Practising Governance

Artificial Intelligence: Model Personal Data Protection Framework

31 October 2024

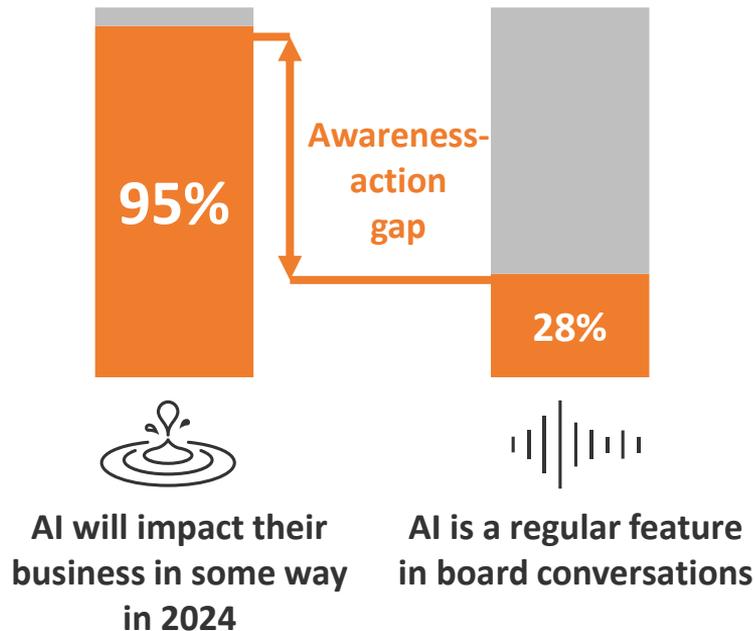
Joyce Liu, Senior Legal Counsel (Acting) &
Head of Global Affairs and Research, PCPD

Ready?

Polls show boards are aware of AI but are not fully engaged

How many directors share the following?

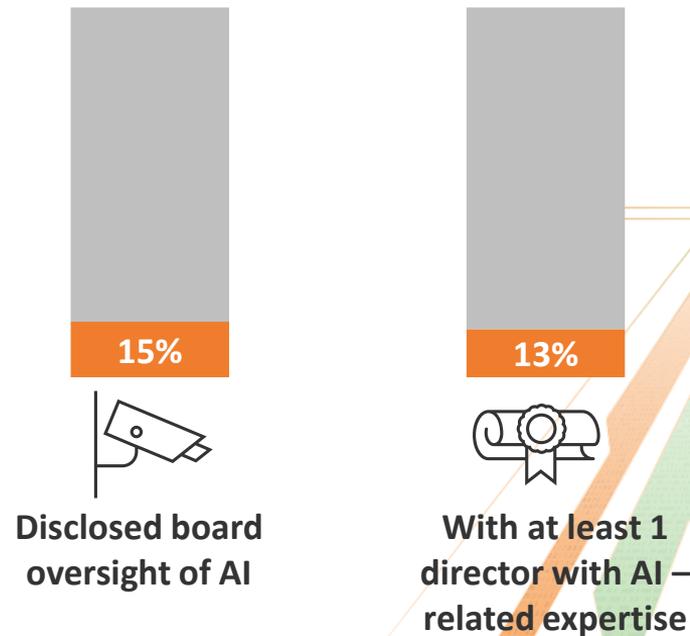
Directors surveyed by NACD, 2023



Source: [National Association of Corporate Directors \(US\)](#)

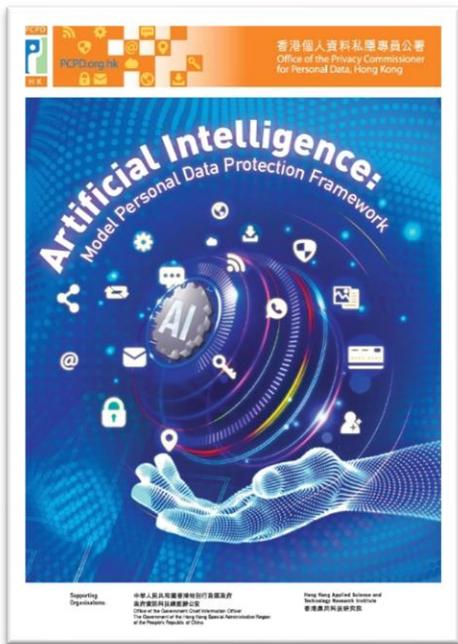
How many listed companies show the following?

S&P 500, Sep 2022 – Sep 2023



Source: [ISS Corporate](#)

Artificial Intelligence: Model Personal Data Protection Framework



Feature

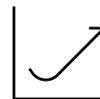


A set of recommendations on the best practices for organisations **procuring, implementing and using any type of AI systems**, including generative AI, that involve the use of personal data

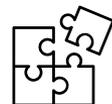
Benefits



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



Nurture the healthy development of AI in Hong Kong

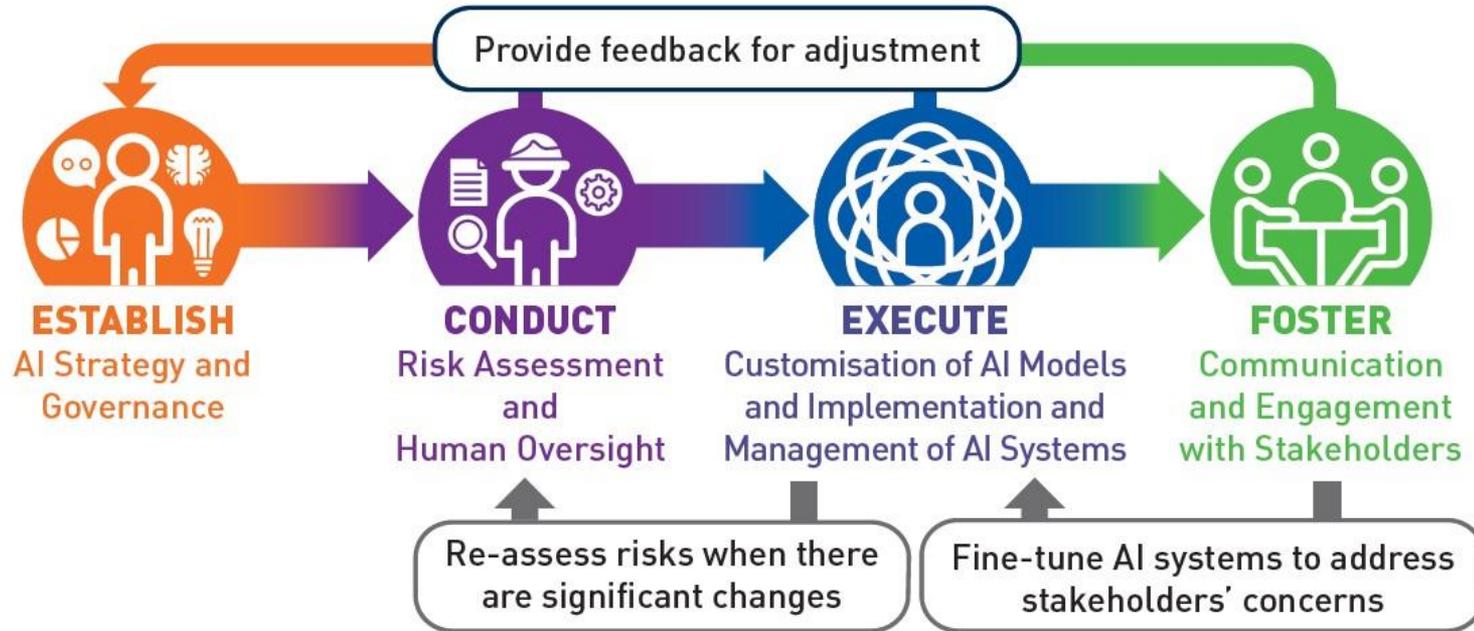


Facilitate Hong Kong's development into an innovation & technology hub



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

Artificial Intelligence: Model Personal Data Protection Framework

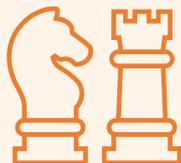


Establish

AI Strategy and Governance

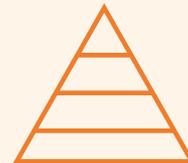


1



AI Strategy

3



Governance
Structure

2



Governance
Considerations

4



Training and
Awareness Raising

AI Strategy

An AI strategy shows management's commitment



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 **the unacceptable uses** of AI systems



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



Establishing **an AI inventory**



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

Governance Considerations

An organisation intending to invest in AI solutions may consider these:



Purpose(s) of using AI

1



Privacy and security obligations and ethical requirements

2



International technical and governance standards

3



Criteria and procedures for reviewing AI solutions

4



Data processor agreements

5



Policy on handling output generated by the AI system

6



Plan for continuously scrutinising changing landscape

7



Plan for monitoring, managing and maintaining AI solution

8

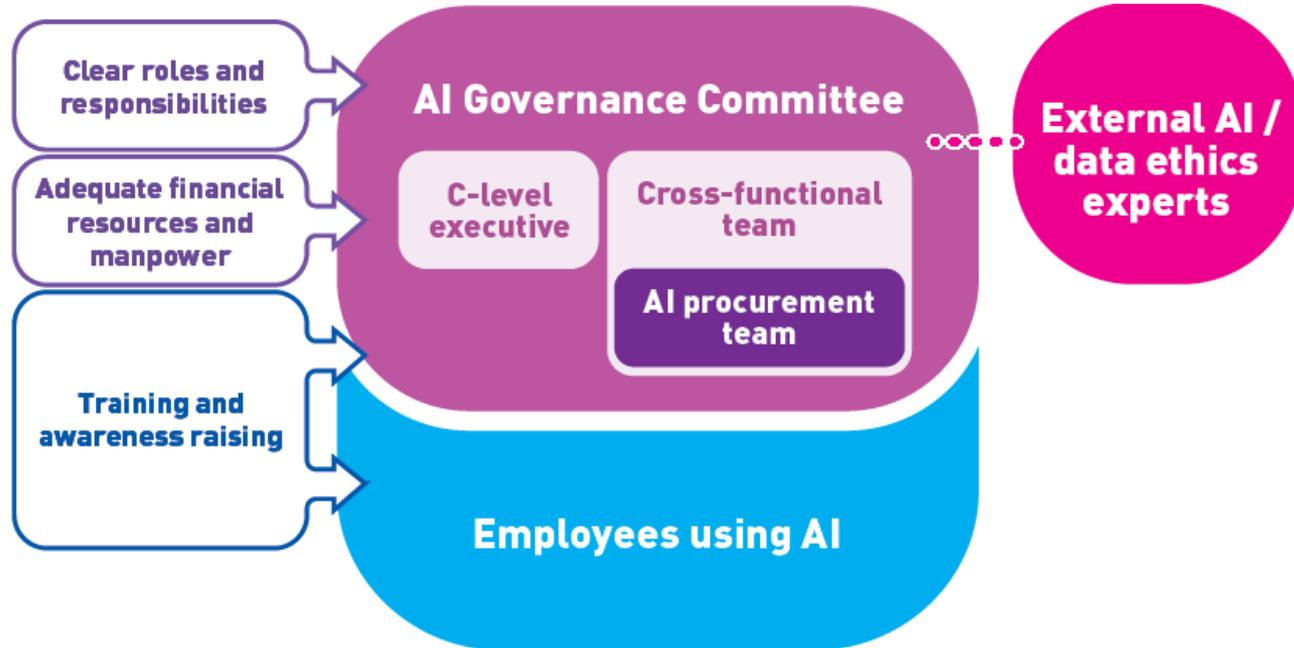


Evaluation of AI supplier

9

Governance Structure

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



Training and Awareness Raising

Different personnel should receive training tailored for them



Recommended Personnel



System analysts/architects / data scientists



AI system users



Legal and compliance professionals



Procurement staff



Human reviewers



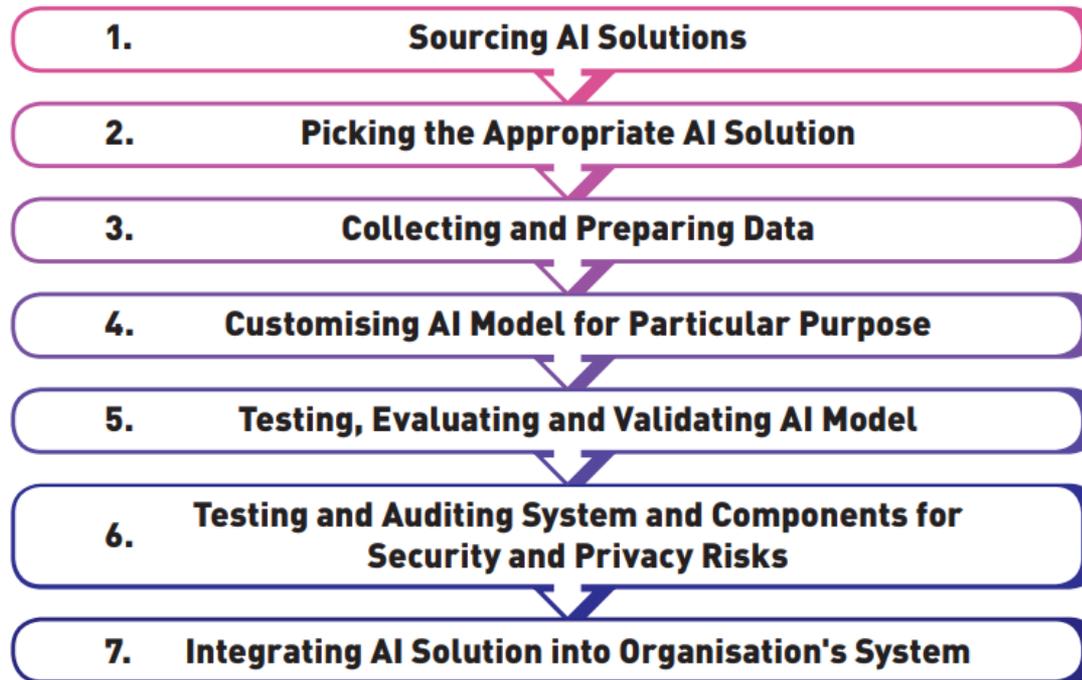
All staff performing work relating to AI system

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

AI procurement steps

AI solution procurement involves 7 steps

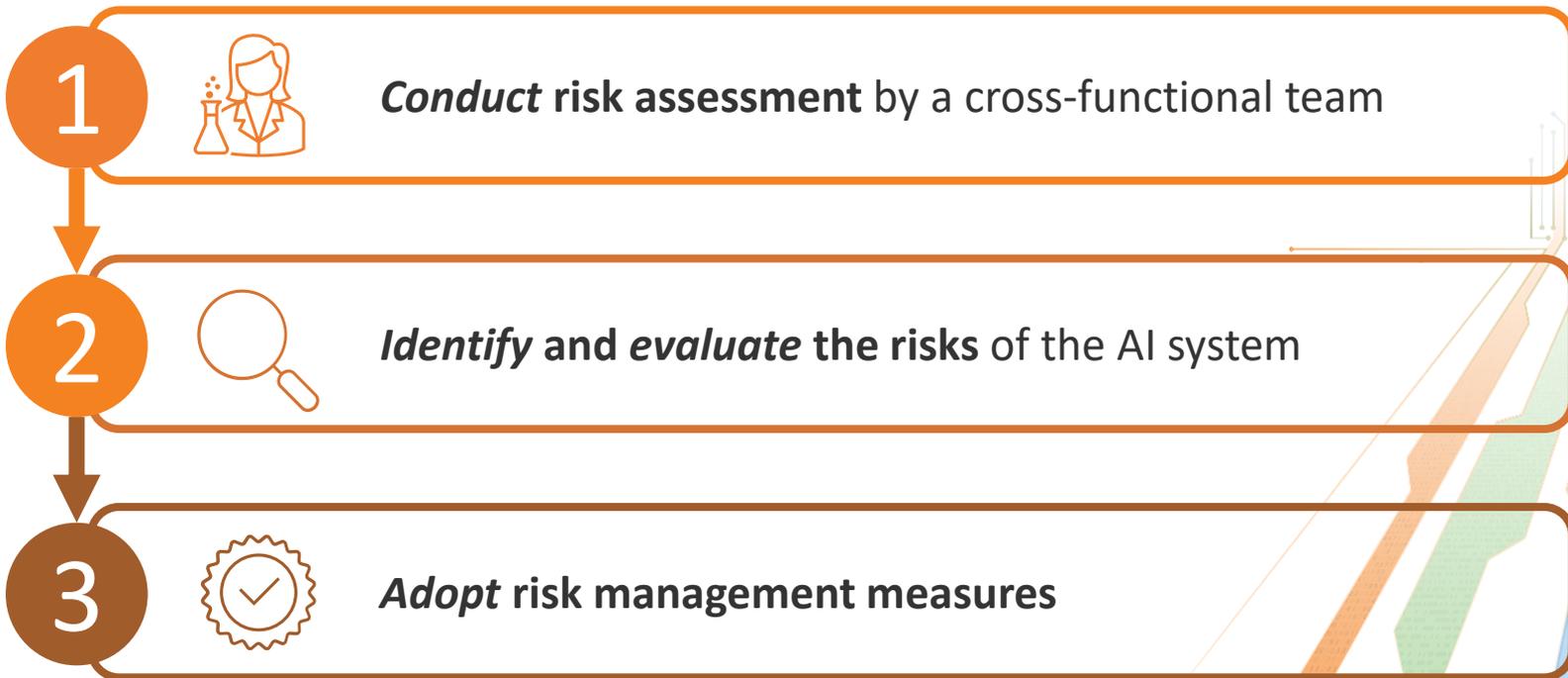


Conduct

Risk assessment and human oversight



Process of Risk Assessment



Risk Factors

Both privacy and ethical risks should be addressed



Risk type

Some factors to consider in a risk assessment

Privacy Risks



- The **allowable uses** of the data
- **Volume** of personal data
- **Sensitivity** of data involved
- **Security** of personal data

Ethical Risks



- **Potential impacts** on the affected individuals, the organisation and the wider community
- **Probability** of impacts of the AI system on individuals, and their **severity** and **duration**

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.



Data Preparation

Compliance, data minimization, quality management, data handling

| Process | Selected Recommendations | |
|--|--|---|
|  <p>Data Preparation</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>Customisation and Implementation of AI</p> |  <p>Conduct rigorous testing and validation of reliability, robustness and fairness</p>  <p>Consider compliance issues based on the hosting of AI solution ('on-premise' or on a third party cloud) prior to integration</p>  <p>Ensure system security and data security</p> | |
|  <p>Management and Continuous Monitoring of AI</p> |  <p>Maintain proper documentation</p>  <p>Establish an AI Incident Response Plan</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

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

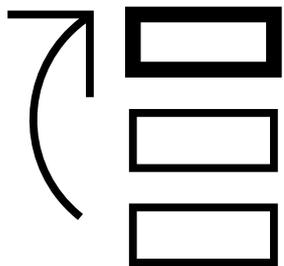
**Data Subject Rights
and Feedback**

4

**Language and
Manner**

Business-friendly

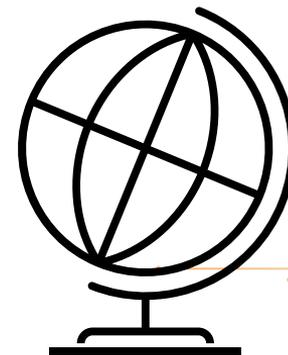
We've designed the Model Framework to be business-friendly



Best practices



Risk-based
Approach



Alignment with
international
standards

PCPD's support

We're here to help



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

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

Supporting
Organisation: 

SME
Hotline

Webinars

Artificial Intelligence: Model Personal Data Protection Framework

that organisations should incorporate into their business process when they procure, implement and use AI

Provide feedback for adjustment

ESTABLISH AI Strategy and Governance

CONDUCT Risk Assessment and Human Oversight

EXECUTE Customisation of AI Models and Implementation and Management of AI Systems

FOSTER Communication and Engagement with Stakeholders

Re-assess risks when there are significant changes

Fine-tune AI systems to address stakeholders' concerns

7 Steps in AI Procurement

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

9 Governance Considerations

1. Purpose of using AI
2. Privacy and security obligations and ethical requirements
3. International technical and governance standards
4. Criteria and procedures for reviewing AI solutions
5. Data processor agreements
6. Policy on handling output generated by the AI system
7. Plan for continuously scrutinising changing landscape
8. Plan for monitoring, managing and maintaining AI solution
9. Evaluation of AI suppliers

Supporting Organisation:  香港應用科技研究院
ASTRI Applied Science and
Technology Research Institute
Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region

2-page leaflet

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

