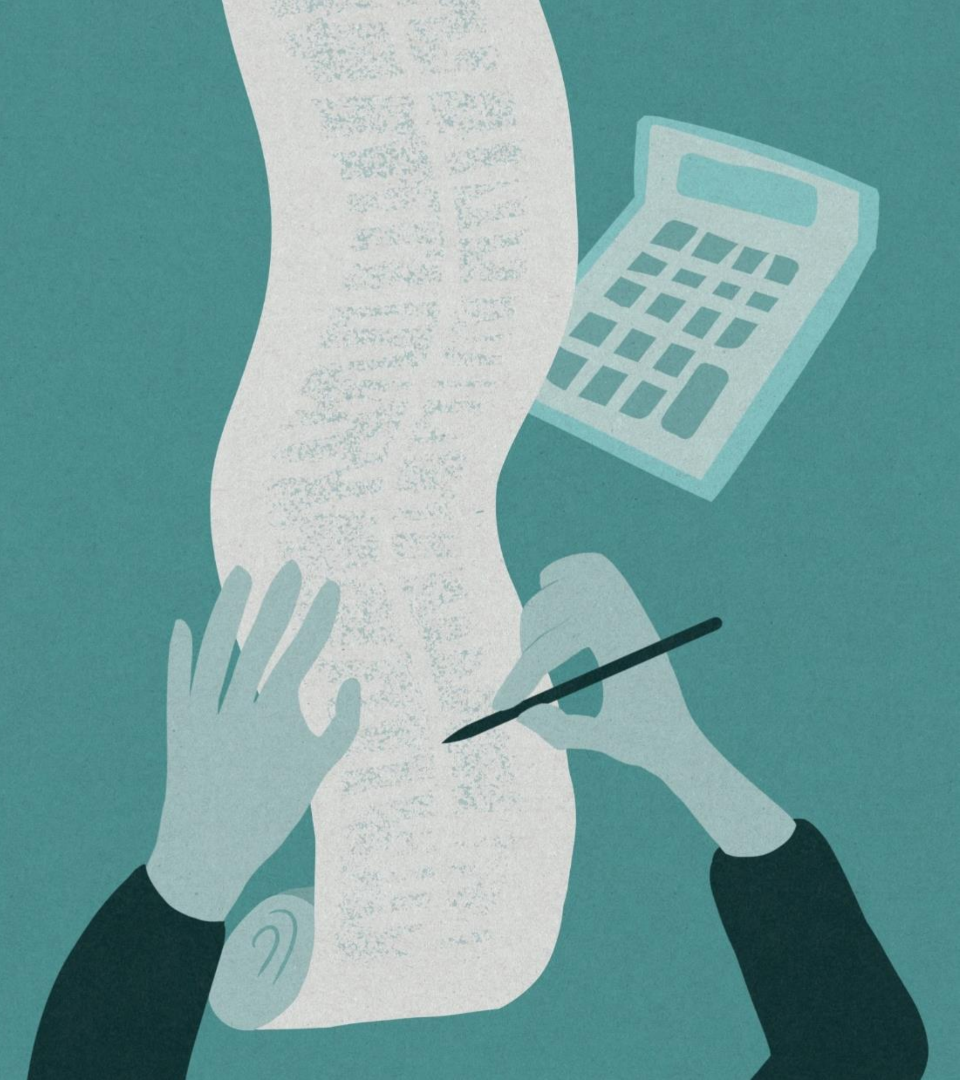


香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

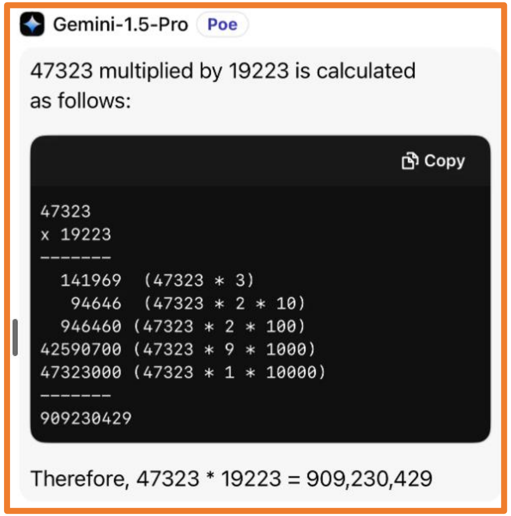
HKICPA IT Conference 2024

AI Governance and Privacy: Best Practices for Accountants

Joyce Liu, Ag. Senior Legal Counsel & Head of Global Affairs and Research, PCPD
9 November 2024

PolyMATH?

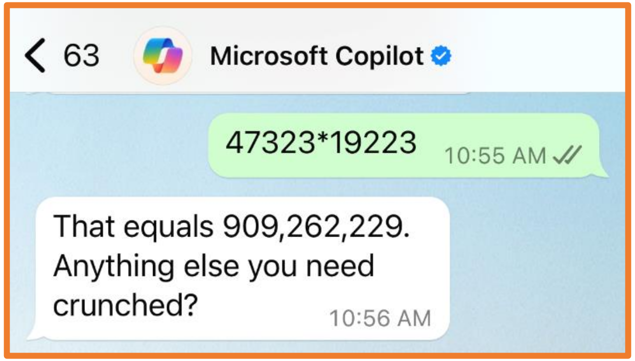
LLMs can do many things, but often struggle with calculations



47323 multiplied by 19223 is calculated as follows:

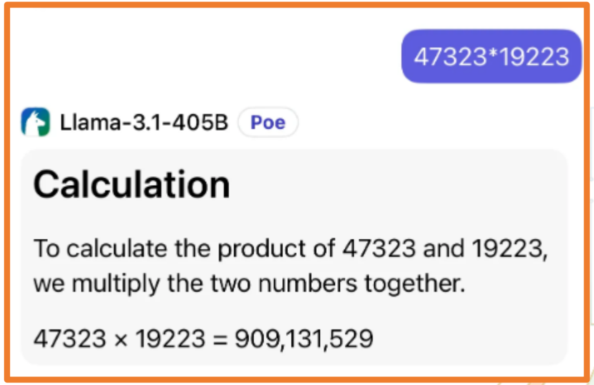
```
47323
x 19223
-------
  141969  (47323 * 3)
   94646  (47323 * 2 * 10)
  946460 (47323 * 2 * 100)
42590700 (47323 * 9 * 1000)
47323000 (47323 * 1 * 10000)
-------
909230429
```

Therefore, 47323 * 19223 = 909,230,429



47323*19223 10:55 AM

That equals 909,262,229. Anything else you need crunched? 10:56 AM

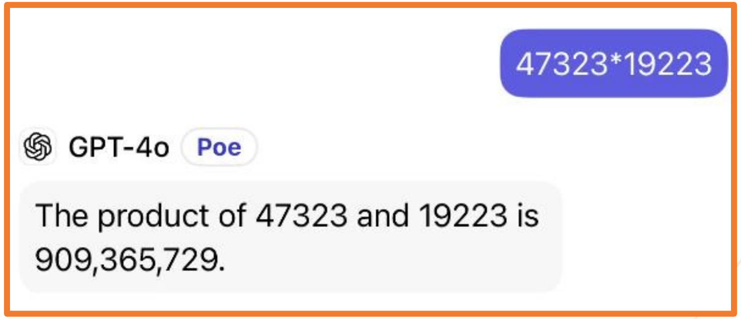


47323*19223

Calculation

To calculate the product of 47323 and 19223, we multiply the two numbers together.

47323 × 19223 = 909,131,529



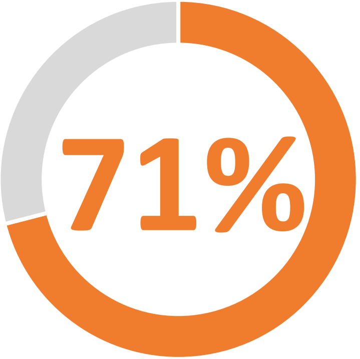
47323*19223

The product of 47323 and 19223 is 909,365,729.

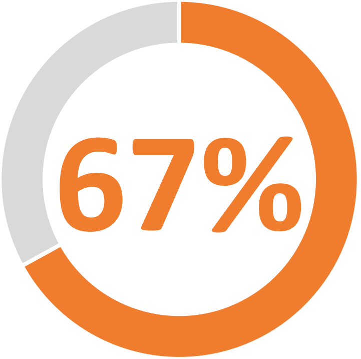
Which one is right?

Statistics

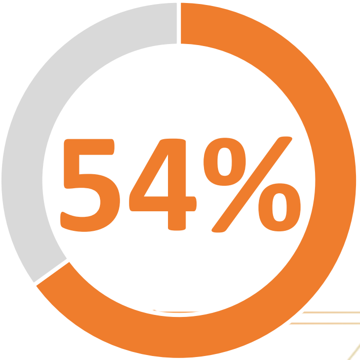
Accountants are quite positive on AI



believe that AI will bring substantial changes to the accounting industry



agree that AI can serve as a competitive advantage



believe that the value of a firm drops if it doesn’t use AI

Source: Karbon

AI Adoption

The accounting industry has been exploring AI to help their work

Task automation

Predictive analytics

Fraud detection

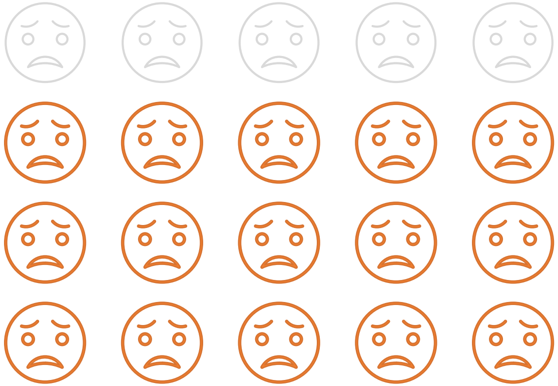
Regulatory compliance

Real-time financial reporting

Enhanced client interactions

Over-optimistic?

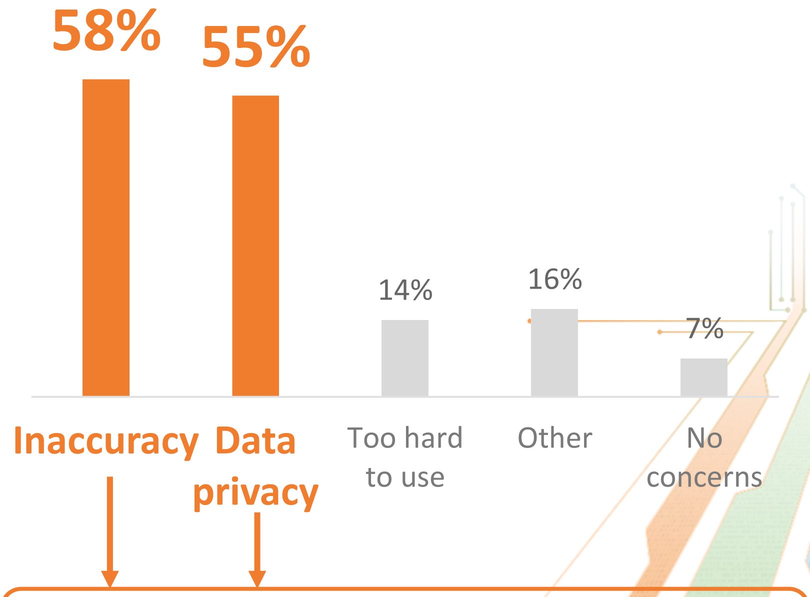
Despite promises, the industry knows it needs to be cautious



76%

of accountants concerned about data security when evaluating AI tools

Source: Karbon



Biggest concerns of accountants about adding AI

Source: Rightworks

Risks

Different risks have arisen from AI

PCPD
H K

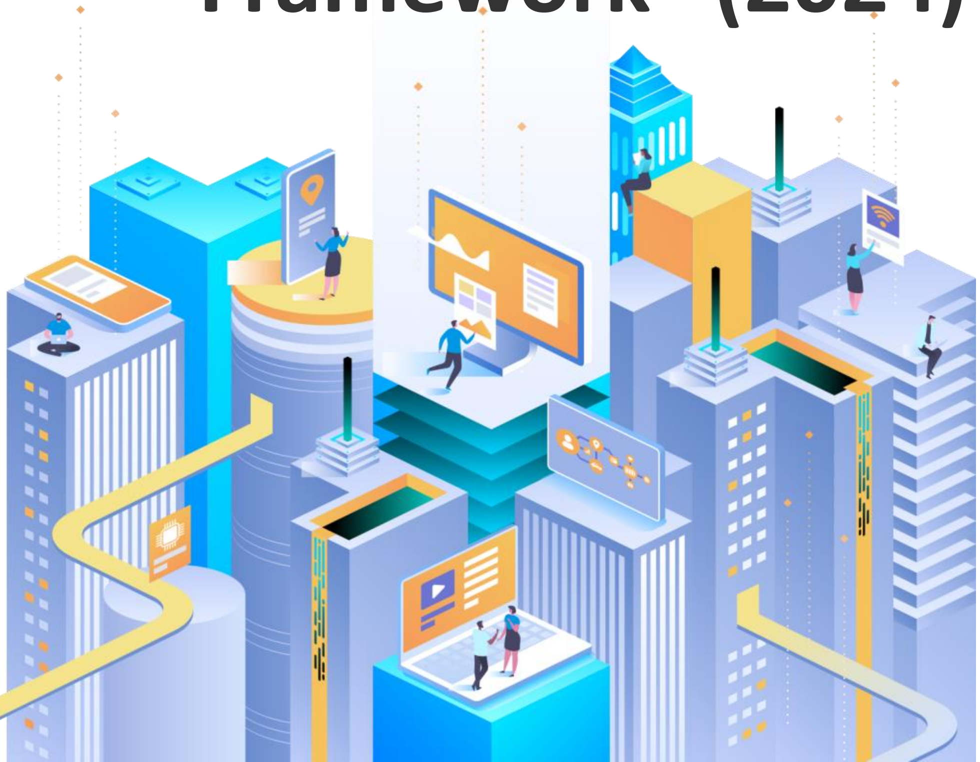
1 Privacy risks

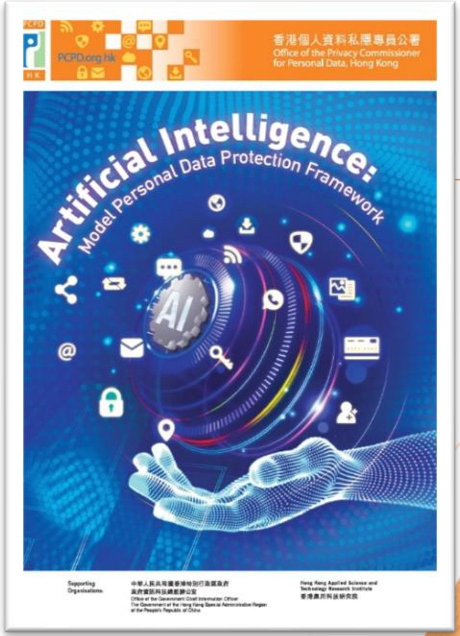
- Excessive data collection
- Misuse of data
- Data security
- Identity re-identification
- Data accuracy

2 Ethical risks

- Interpretation of decisions
- Harmful content
- Copyright issues
- Bias and inaccuracies
- Hallucination

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





PCPD.org.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

Supporting Organisations

中華人民共和國香港特別行政區政府
政府資訊科技總監辦公室
Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Hong Kong Applied Science and Technology Research Institute
香港應用科技研究院

International standards

The Framework aligns with internationally recognised values and principles

Guidance on the Ethical Development and Use of Artificial Intelligence

PCPD.org.hk

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

3 Data Stewardship Values

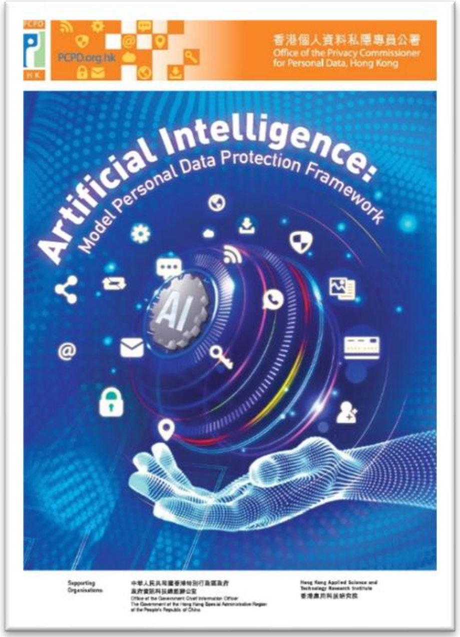
1. Being respectful
2. Being beneficial
3. Being fair

7 Ethical Principles for AI

1. Accountability
2. Human oversight
3. Transparency & interpretability
4. Data Privacy
5. Fairness
6. Beneficial AI
7. Reliability, robustness & security

Model Personal Data Protection Framework

Artificial Intelligence: Model Personal Data Protection Framework



PCPD.org.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

Supporting Organisations

中華人民共和國香港特別行政區政府
政府資訊科技總監辦公室
Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Hong Kong Applied Science and Technology Research Institute
香港應用科技研究院

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

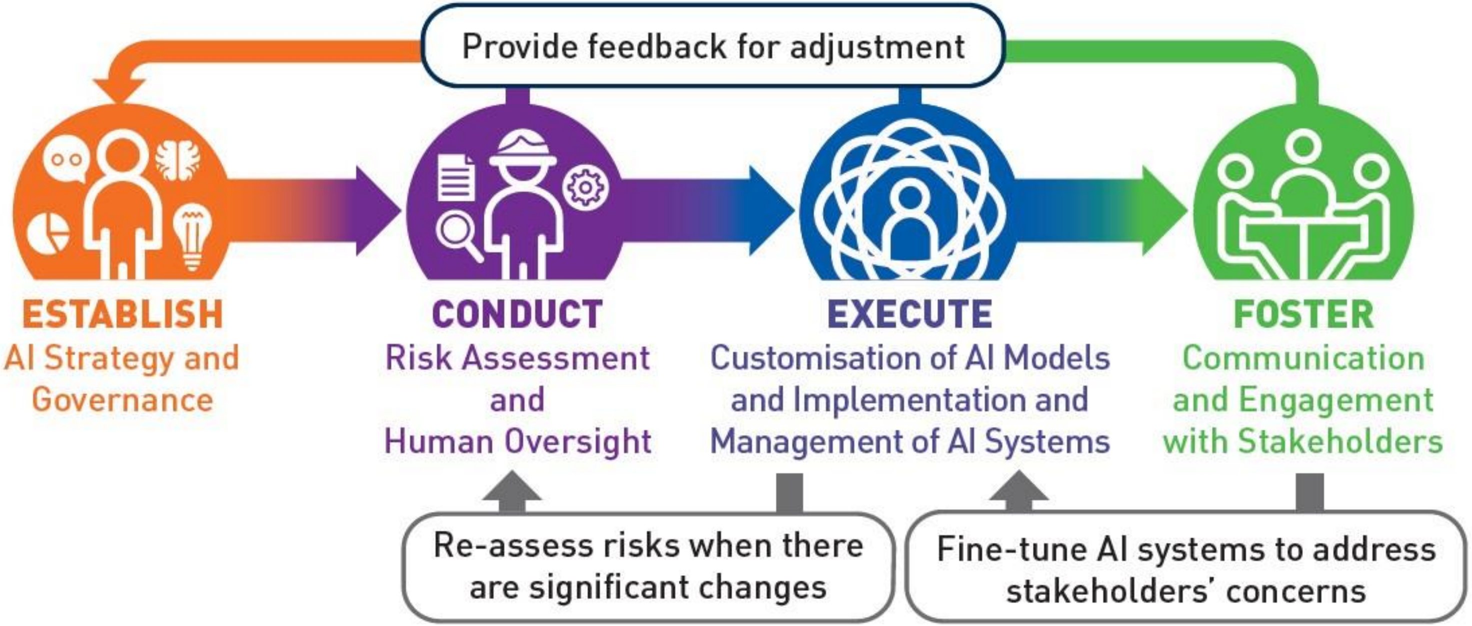
Assist organisations in complying with the requirements of the Personal Data (Privacy) Ordinance

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



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

AI Strategy

An AI strategy shows management’s commitment

ESTABLISH
AI Strategy and Governance

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

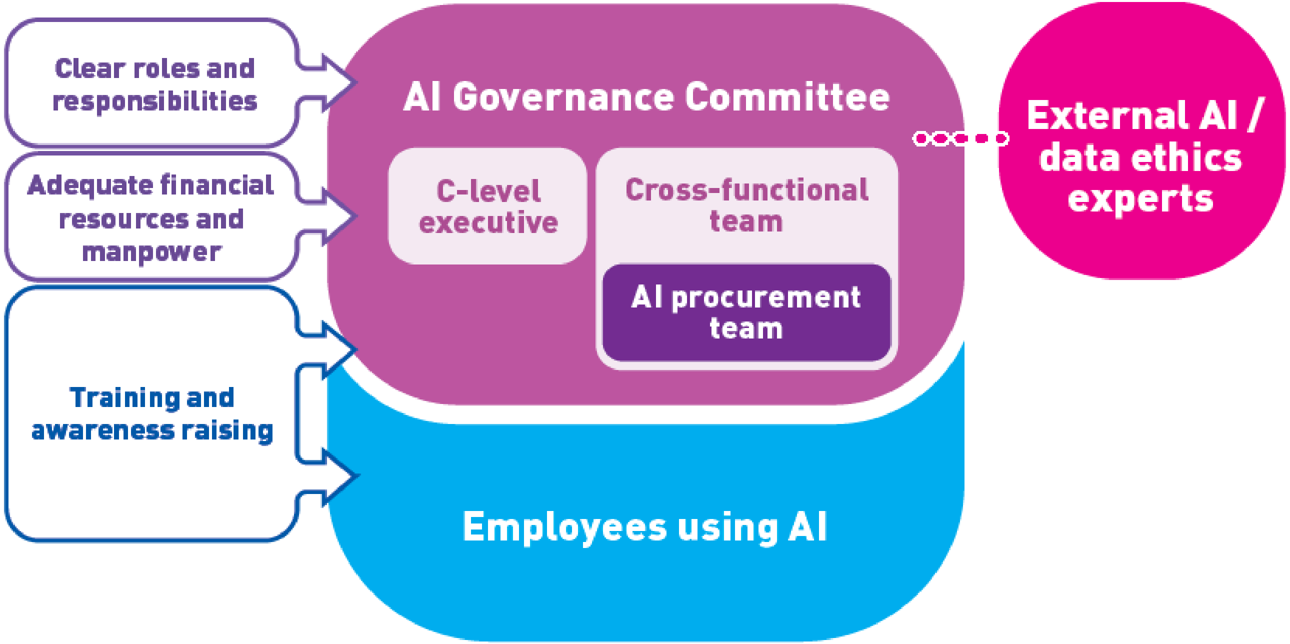
Elements that may be included

- Setting out **ethical principles**
- Determining the **unacceptable uses** of AI systems
- Establishing an **AI inventory**
- Establishing **specific internal policies and procedures**
- Regularly **communicating the AI strategy,** policies and procedures
- Considering **emerging laws and regulations** that may be applicable

Governance Structure

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

ESTABLISH
AI Strategy and Governance



Clear roles and responsibilities

Adequate financial resources and manpower

Training and awareness raising

AI Governance Committee

C-level executive

Cross-functional team

AI procurement team

External AI / data ethics experts

Employees using AI

7 Steps for AI Procurement and Implementation

The flowchart shows the general process

ESTABLISH
AI Strategy and Governance

1. Source AI solutions
2. Pick the appropriate AI solution
3. Collect and prepare data
4. Customise AI model for particular purpose
5. Test, evaluate and validate AI model
6. Test and audit system and components for security and privacy risks
7. Integrate AI solution into organisation's system

Governance Considerations

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

ESTABLISH
AI Strategy and Governance

1. Purpose(s) 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 supplier

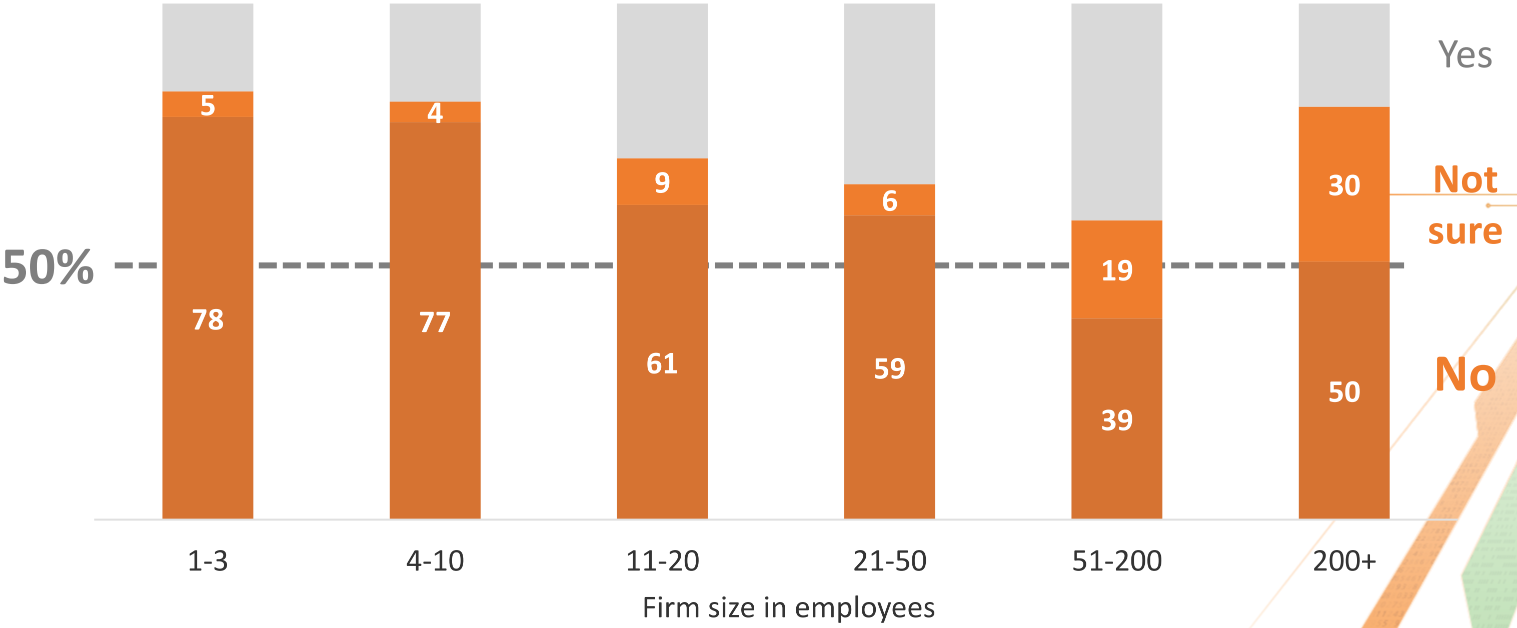
Training and Awareness Raising

Regardless of firm size, AI training is uncommon among accounting firms

ESTABLISH
AI Strategy and Governance

Is AI training offered at your firm?

%, by firm size



Source: Karbon

Training and Awareness Raising

Different personnel should receive training tailored for them

ESTABLISH
AI Strategy and Governance

Recommended Personnel	Training Topics
System analysts/architects / data scientists	• Compliance with data protection laws, regulations and internal policies; cybersecurity risks
AI system users	• Compliance with data protection laws, regulations and internal policies; cybersecurity risks; general AI technology
Legal and compliance professionals	• General AI technology and governance
Procurement staff	• General AI technology and governance
Human reviewers	• Detection and rectification of any unjust bias, unlawful discrimination and errors / inaccuracies in the decisions made by AI systems or presented in the content
All staff performing work relating to AI system	• Benefits, risks, functions and limitations of the AI system(s) used by the organisation

Conduct

Risk assessment and human oversight

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 Factors

Both privacy and ethical risks should be addressed

CONDUCT
Risk Assessment
and
Human Oversight

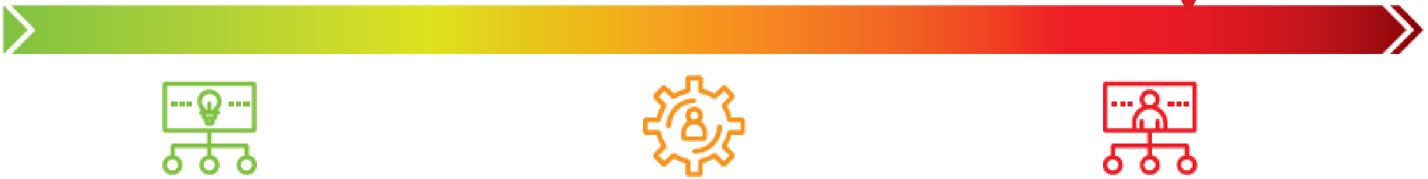
Risk type	Some factors to consider in a risk assessment
Privacy Risks	- The **allowable uses** of the data - **Volume** of personal data - **Sensitivity** of data involved - **Security** of personal data
Ethical Risks	- **Potential impacts** on the affected individuals, the organisation and the wider 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

CONDUCT
Risk Assessment
and
Human Oversight

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



Lower — ***Risk level of AI system*** — *Higher*

Human-out-of-the-loop
AI makes decisions without human intervention

Human-in-command
Human actors oversee the operation of AI and intervene whenever necessary

Human-in-the-loop
Human actors retain control in the decision-making process

Execute

Customisation of AI Models and implementation and management of AI systems

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

Process	Selected Recommendations
Data Preparation	Ensure compliance with privacy law Minimise the amount of personal data involved Manage data quality Document data handling
Customisation and Implementation of AI	Conduct rigorous testing and validation of reliability, robustness and fairness Consider compliance issues based on the hosting of AI solution (‘on-premise’ or on a third party cloud) prior to integration Ensure system security and data security
Management and Continuous Monitoring of AI	Maintain proper documentation **Establish an AI Incident Response Plan** Conduct periodic audits Consider incorporating review mechanisms as risk factors evolve

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

Image source: Wikimedia Commons (no changes made)

Foster

Communication and Engagement with Stakeholders

FOSTER
Communication
and Engagement
with Stakeholders

1 **Information Provision**

2 **Data Subject Rights and Feedback**

3 **Explainable AI**

4 **Language and Manner**

Benefits

Appropriate use of AI could benefit the industry

Enhanced Efficiency and Accuracy

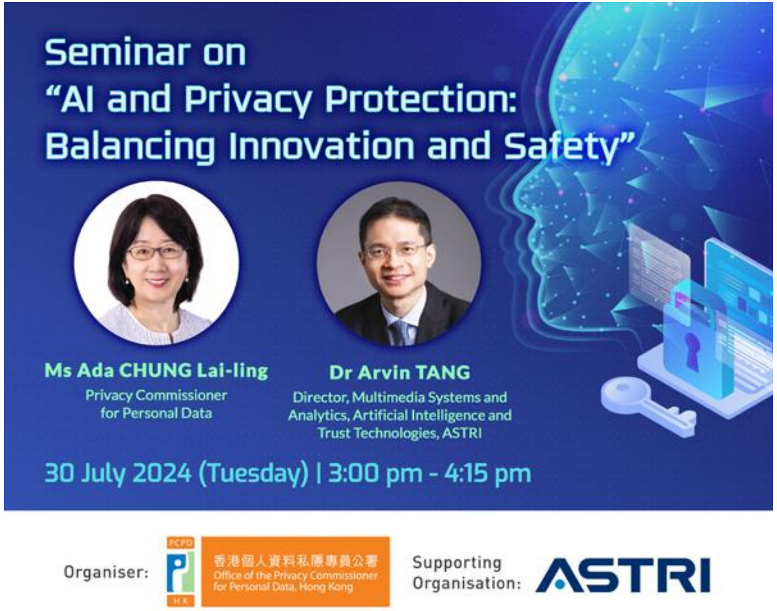
Improved Customer Experience

Increased Job Satisfaction

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

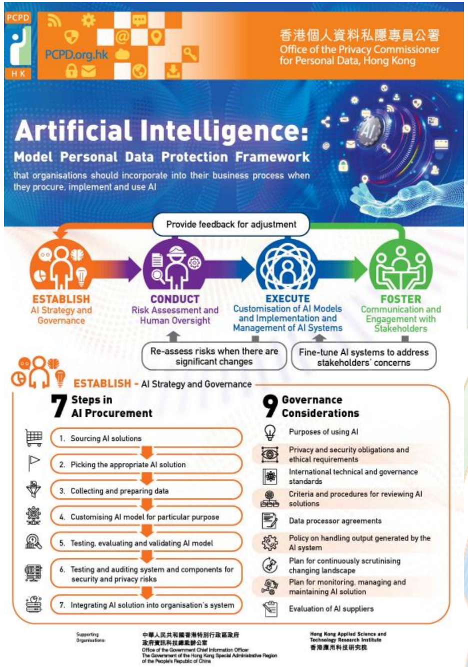
Dr Arvin TANG
Director, Multimedia Systems and Analytics, Artificial Intelligence and Trust Technologies, ASTRI

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

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: ASTRI

Webinars



PCPD.org.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

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

ESTABLISH - AI Strategy and Governance

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

- Purposes 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 suppliers

Supporting Organisations:
中華人民共和國香港特別行政區政府
政府資訊科技總監辦公室
Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

Hong Kong Applied Science and Technology Research Institute
香港應用科技研究院

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

Please Follow Us