PCPD

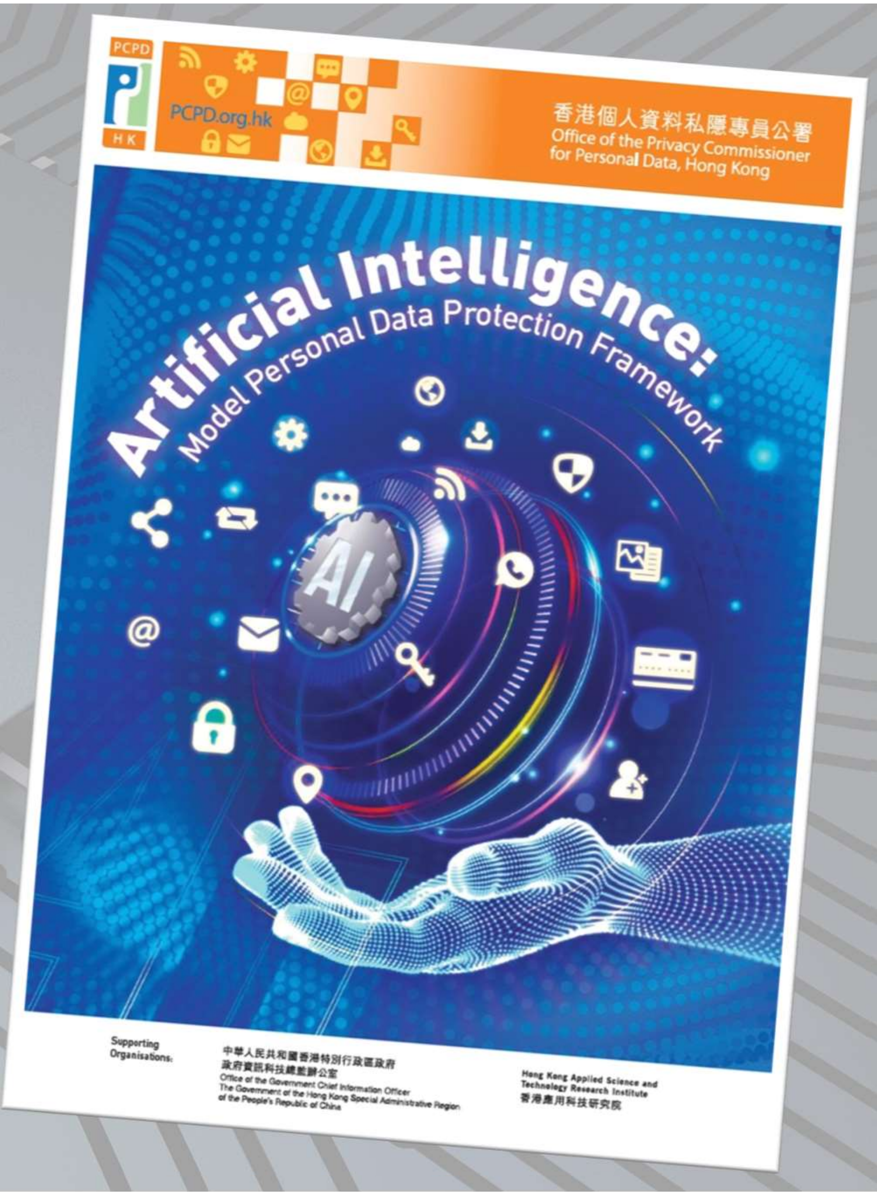
HK

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

Artificial Intelligence and Personal Data Protection: Best Practices and Recommendations

Cecilia SIU

Assistant Privacy Commissioner
for Personal Data (Legal, Global
Affairs and Research)



PCPD

HK

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

Guidance on the Ethical Development and Use of Artificial Intelligence (2021)

3 Data Stewardship Values

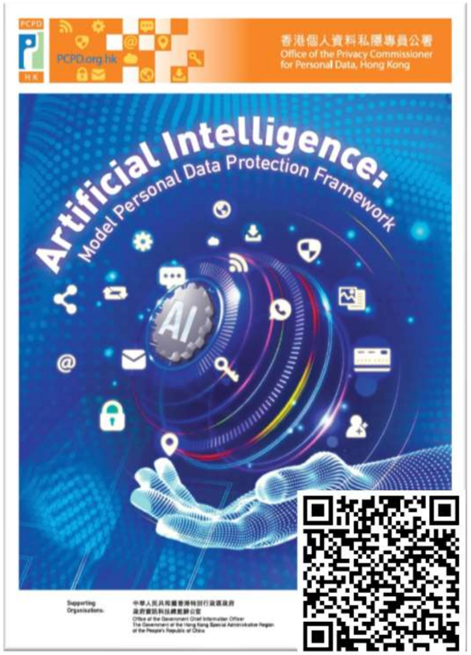
1. Being Respectful
2. Being Beneficial
3. Being Fair

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

Guidance on the Ethical Development and Use of
Artificial Intelligence

Artificial Intelligence:
Model Personal Data Protection Framework (Jun 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

✨ Feature

Recommendations and 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

Supporting organisations, Consultation and References

Supporting Organisations

- **Office of the Government Chief Information Officer (OGCIO), now Digital Policy Office (DPO)**
- **Hong Kong Applied Science and Technology Research Institute (ASTRI)**

Consultation

- PCPD's Standing Committee on Technological Developments

Public bodies

Industry associations

Universities

AI suppliers

International References

Guidance & publications of international bodies, governmental bodies, other data protection authorities

Reports by relevant professional industries

International Standards

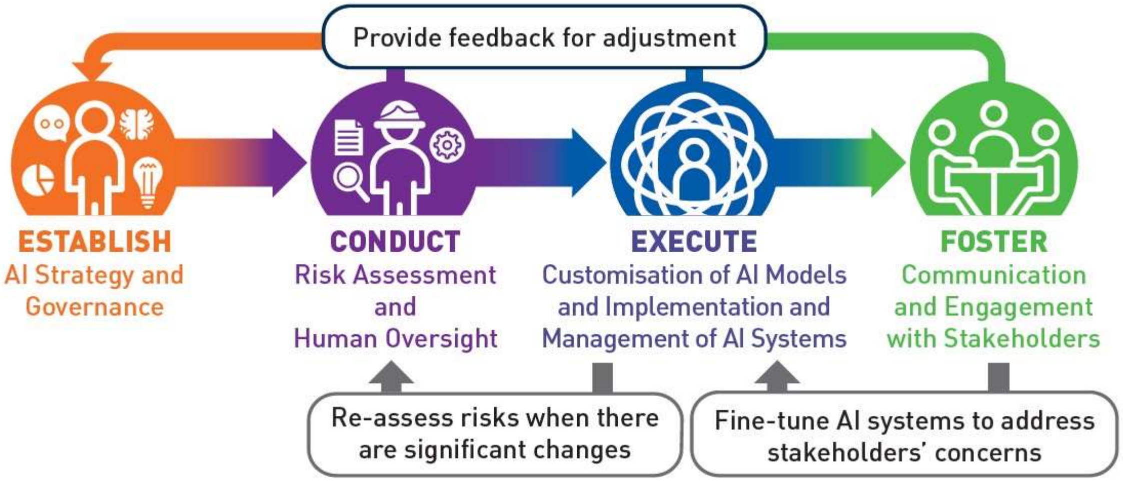
3 Data Stewardship Values

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



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

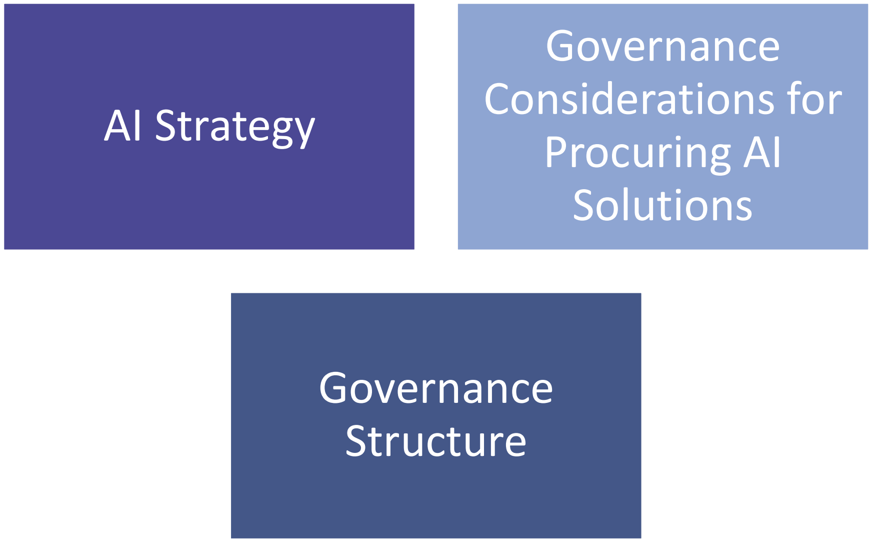
FOSTER
Communication and Engagement with Stakeholders

Re-assess risks when there are significant changes

Fine-tune AI systems to address stakeholders' concerns

1. Establish AI Strategy and Governance

AI Governance Strategy

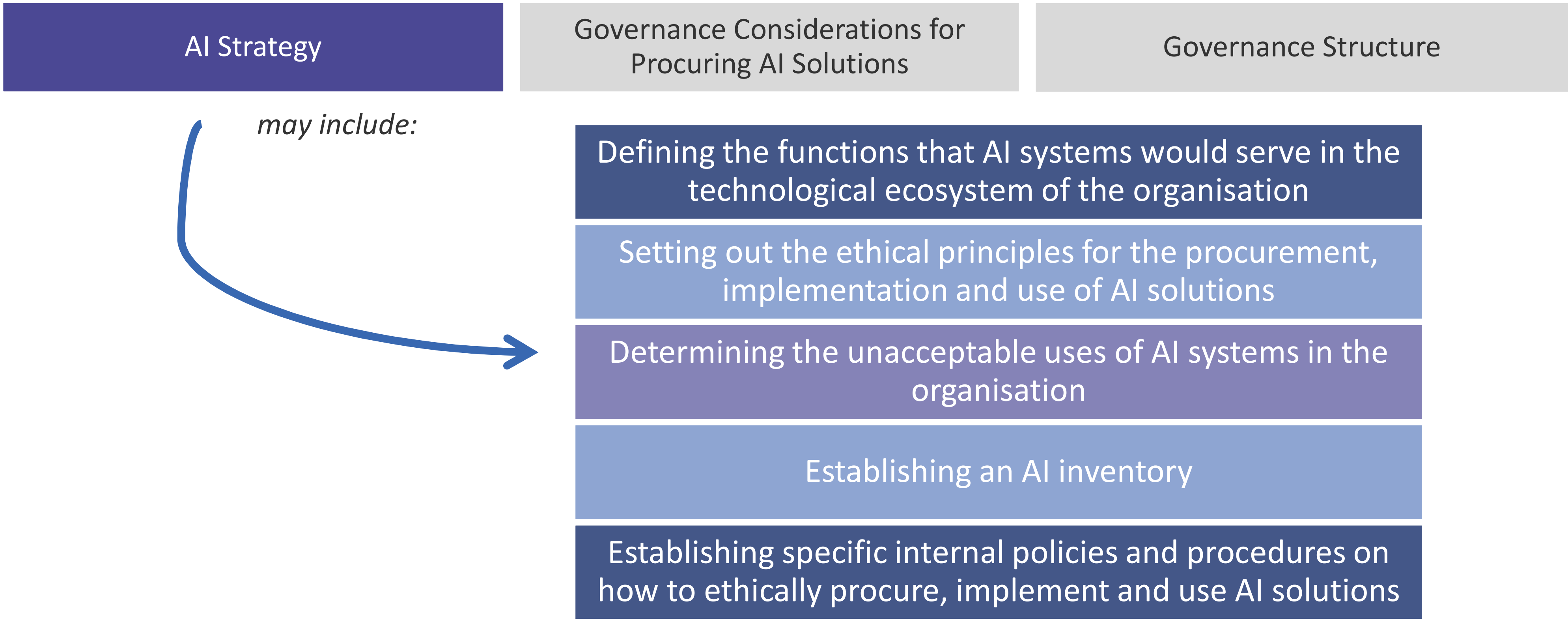


AI Strategy

Governance Considerations for Procuring AI Solutions

Governance Structure

1. Establish AI Strategy and Governance



AI Strategy

Governance Considerations for Procuring AI Solutions

Governance Structure

may include:

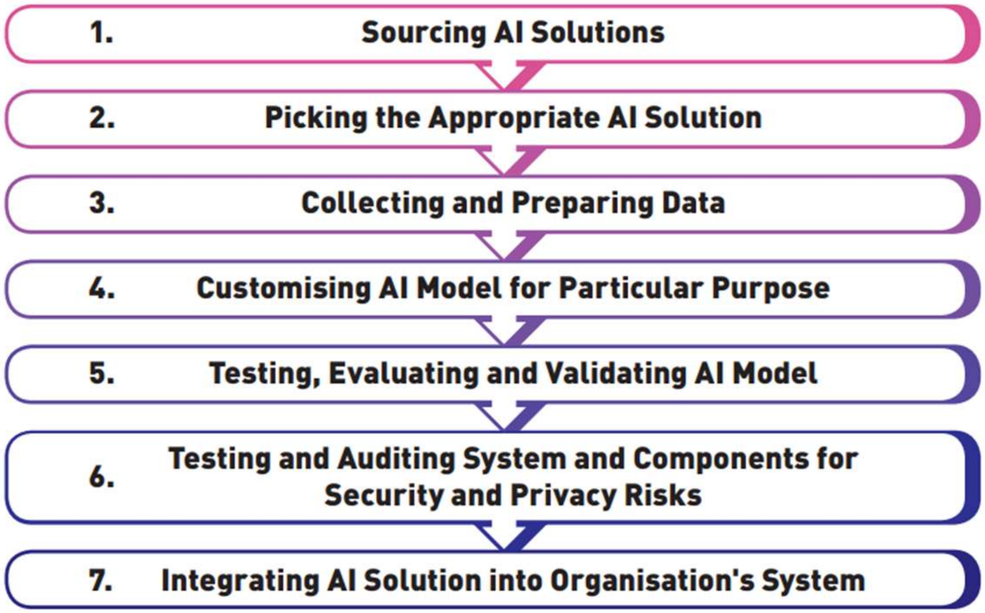
- Defining the functions that AI systems would serve in the technological ecosystem of the organisation
- Setting out the ethical principles for the procurement, implementation and use of AI solutions
- Determining the unacceptable uses of AI systems in the organisation
- Establishing an AI inventory
- Establishing specific internal policies and procedures on how to ethically procure, implement and use AI solutions

1. Establish AI Strategy and Governance

AI Strategy

Governance Considerations for Procuring AI Solutions

Governance Structure



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

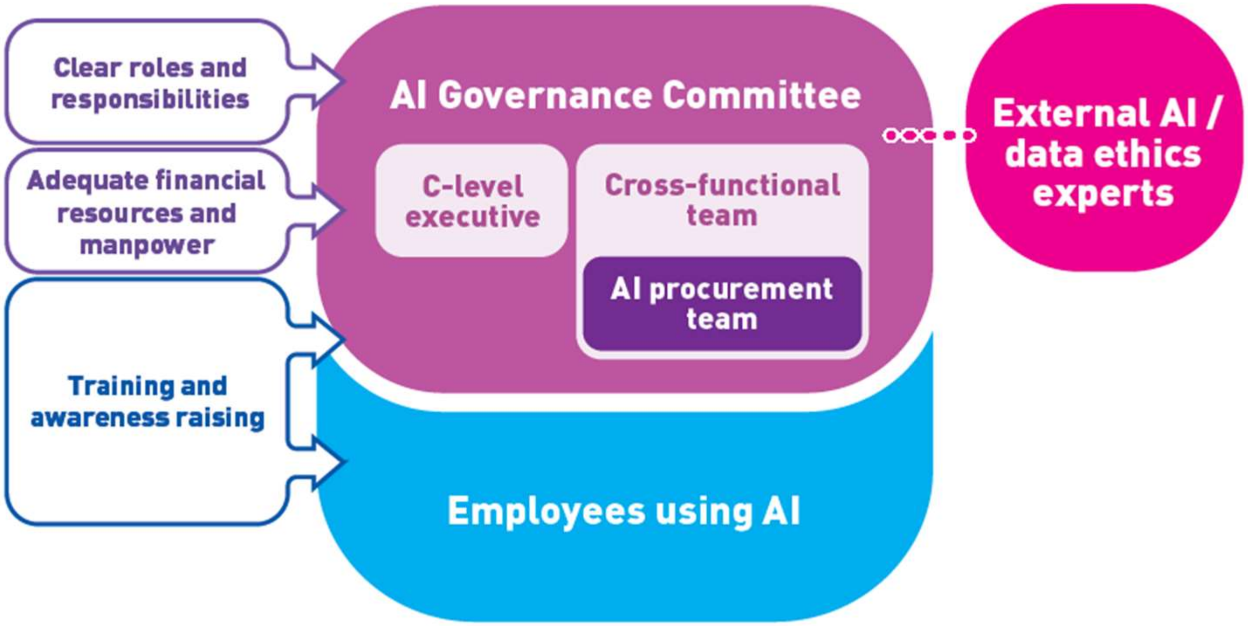
1. Establish AI Strategy and Governance

🤔 9 Governance Considerations

- 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

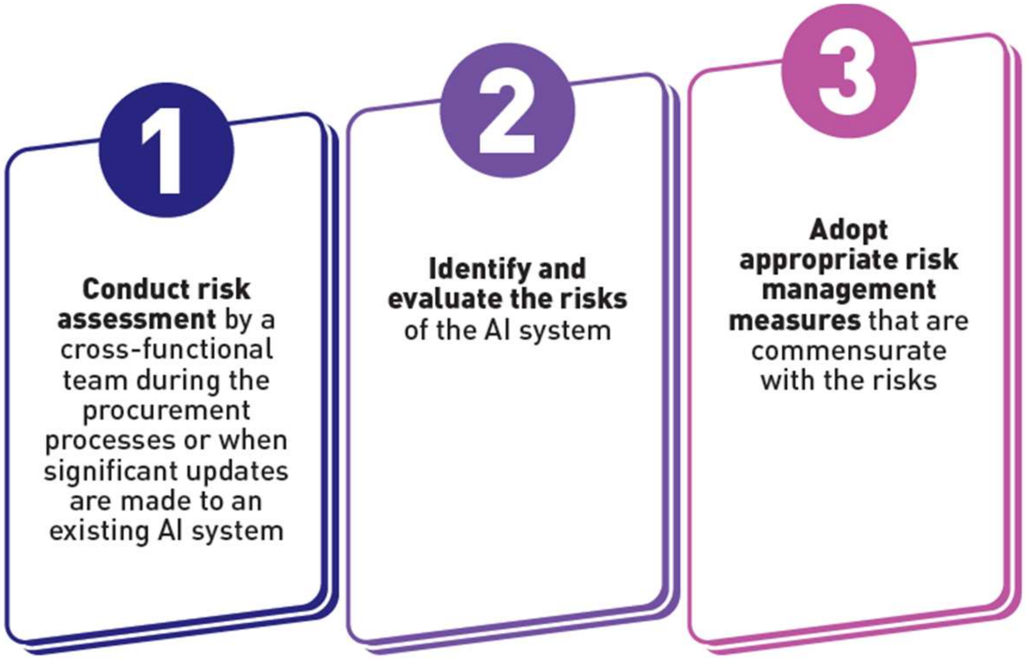
1. Establish AI Strategy and Governance

AI Strategy	Governance Considerations for Procuring AI Solutions	Governance Structure


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

2. Conduct Risk Assessment and Human Oversight

Process of Risk Assessment



1

Conduct risk assessment by a cross-functional team during the procurement processes or when significant updates are made to an existing AI system

2

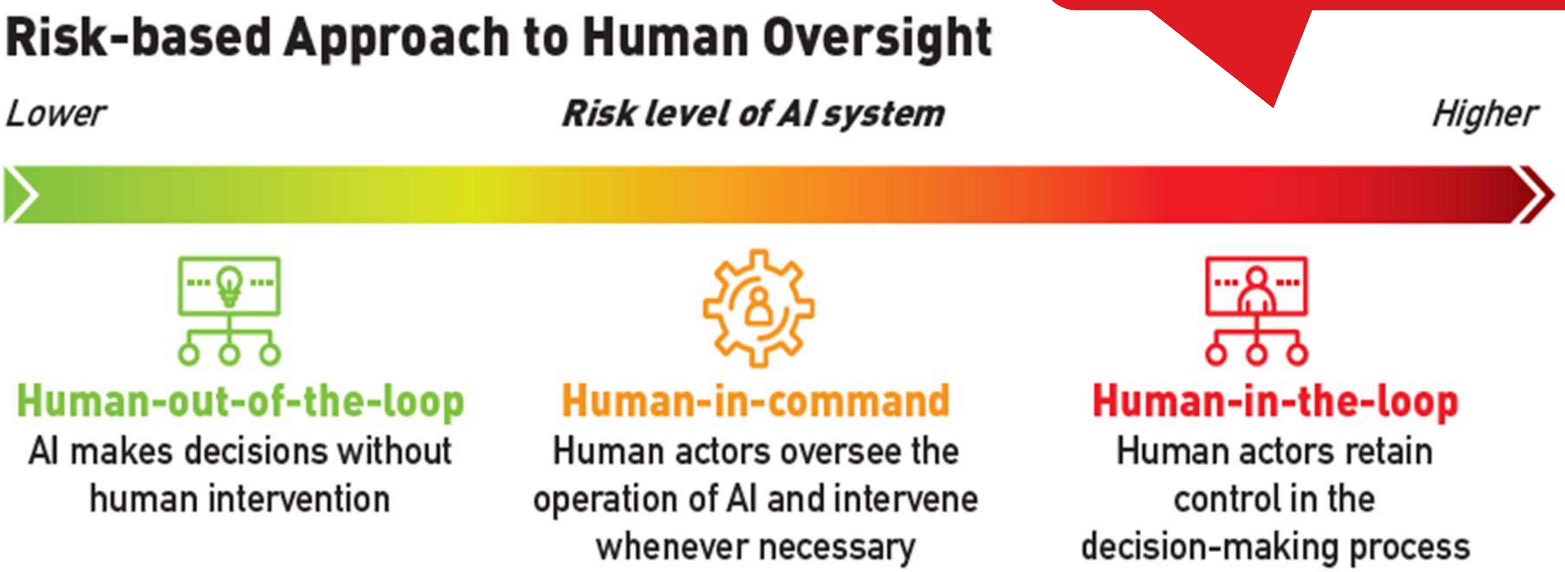
Identify and evaluate the risks of the AI system

3

Adopt appropriate risk management measures that are commensurate with the risks

2. Conduct Risk Assessment and Human Oversight

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



Risk-based Approach to Human Oversight

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

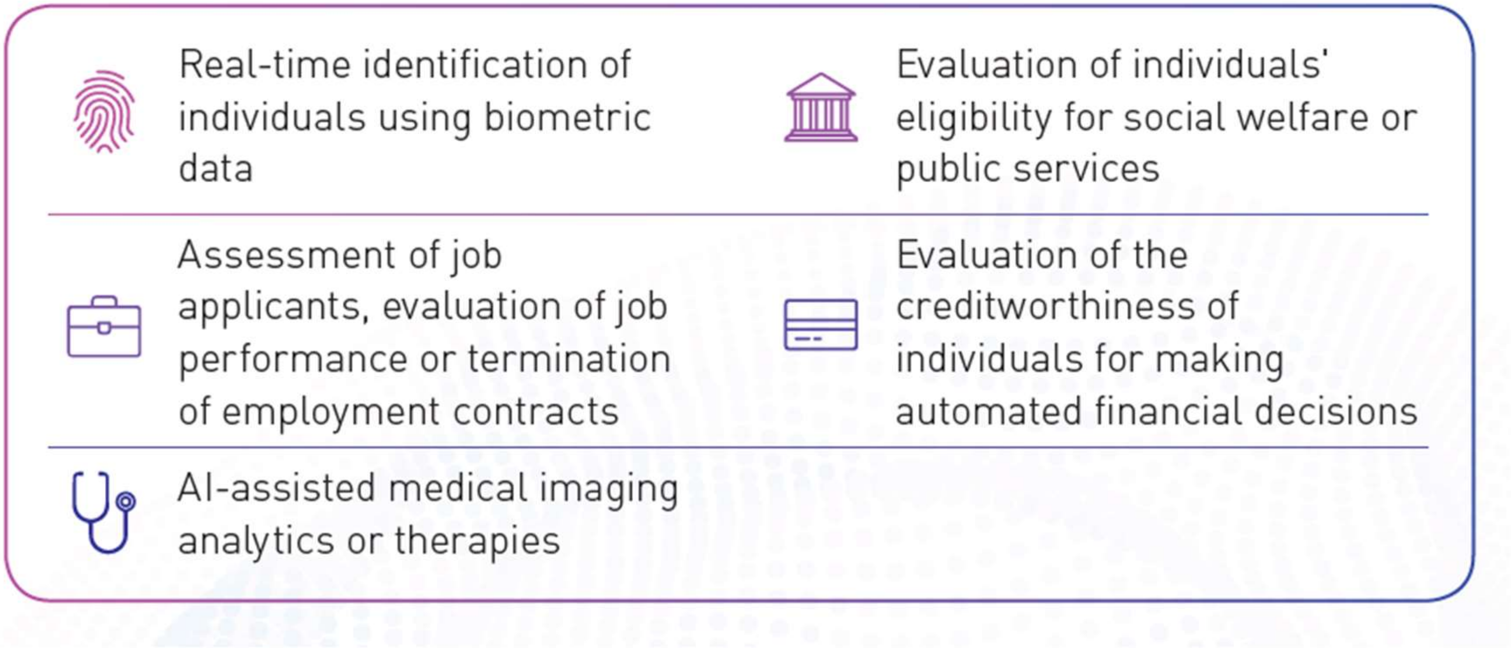
Human-out-of-the-loop
AI makes decisions without human intervention

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

2. Conduct Risk Assessment and Human Oversight

Examples of AI Use Cases that May Incur Higher Risk



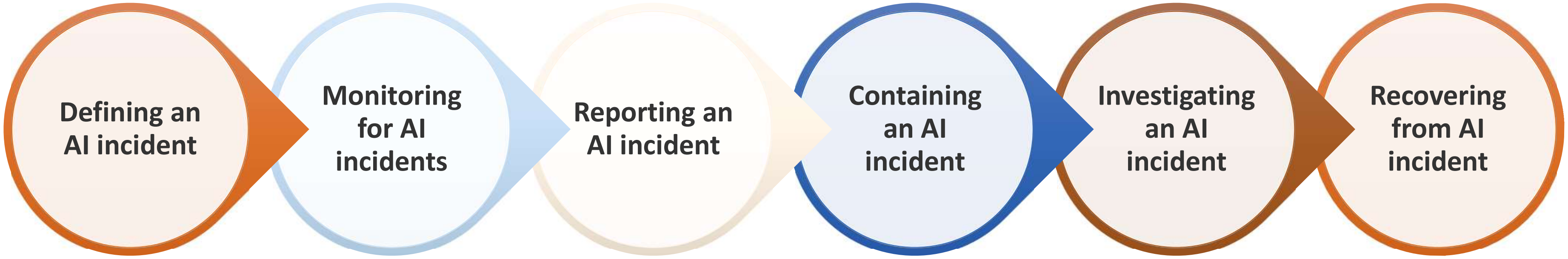
- Real-time identification of individuals using biometric data
- Evaluation of individuals' eligibility for social welfare or public services
- Assessment of job applicants, evaluation of job performance or termination of employment contracts
- Evaluation of the creditworthiness of individuals for making automated financial decisions
- AI-assisted medical imaging analytics or therapies

3. 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

3. Execute Customisation of AI Models and Implementation and Management of AI Systems

AI Incident Response Plan


Defining an AI incident

Monitoring for AI incidents

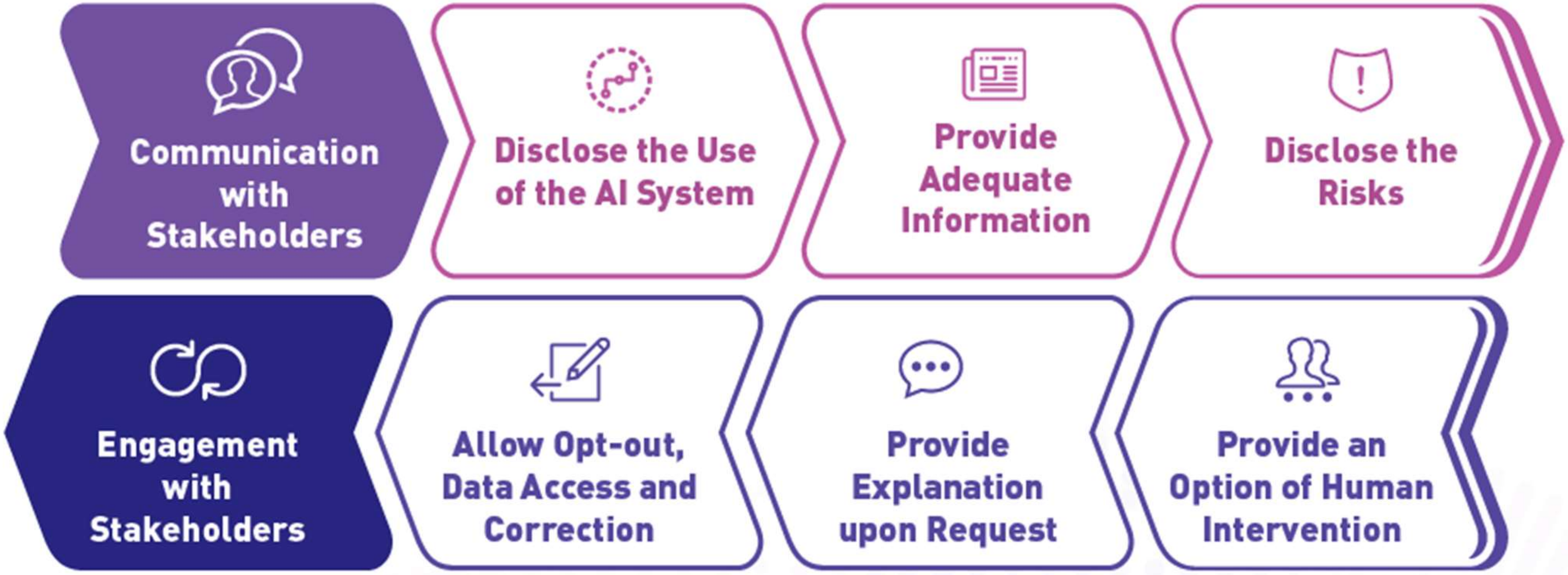
Reporting an AI incident

Containing an AI incident

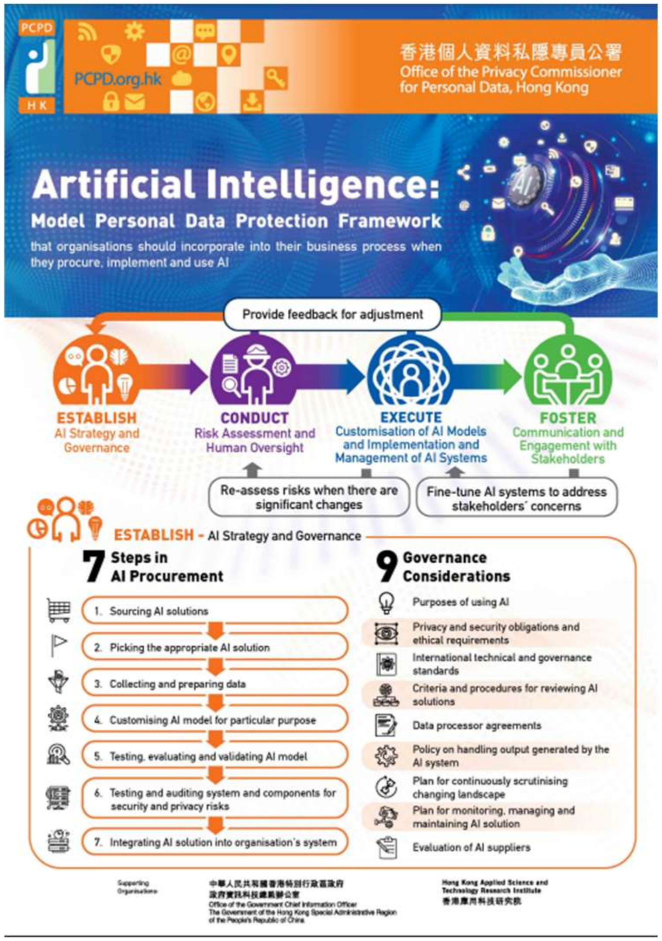
Investigating an AI incident

Recovering from AI incident

4. Foster Communication and Engagement with Stakeholders


Communication with Stakeholders
Disclose the Use of the AI System
Provide Adequate Information
Disclose the Risks
Engagement with Stakeholders
Allow Opt-out, Data Access and Correction
Provide Explanation upon Request
Provide an Option of Human Intervention

Leaflet



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

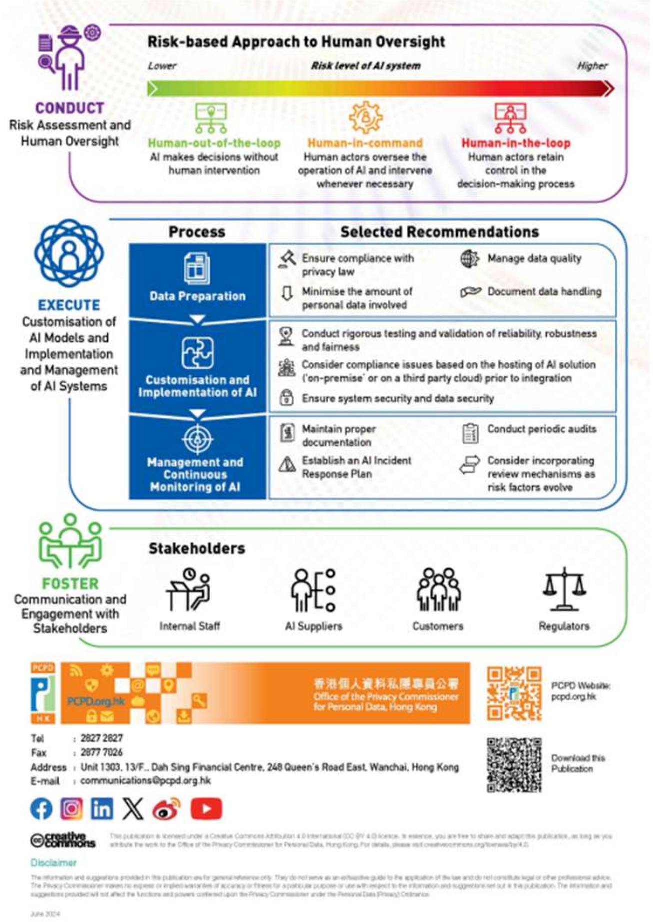
9 Governance Considerations

- 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



CONDUCT
Risk Assessment and Human Oversight

Risk-based Approach to Human Oversight

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

Human-out-of-the-loop	Human-in-command	Human-in-the-loop
AI makes decisions without human intervention	Human actors oversee the operation of AI and intervene whenever necessary	Human actors retain control in the decision-making process

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

Process	Selected Recommendations
Data Preparation	Ensure compliance with privacy law Manage data quality Minimise the amount of personal data involved 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 Conduct periodic audits Establish an AI Incident Response Plan Consider incorporating review mechanisms as risk factors evolve

FOSTER
Communication and Engagement with Stakeholders

Stakeholders

Internal Staff | AI Suppliers | Customers | Regulators

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

PCPD Website: pcpd.org.hk

Download this Publication

Tel : 2827 2827
Fax : 2877 7026
Address : Unit 1303, 13/F., Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong
E-mail : communications@pcpd.org.hk

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law and do not constitute legal or other professional advice. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

June 2024

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