

PCPD



H K

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

IAPP Hong Kong KnowledgeNet Chapter Event: AI Governance Approach for MNCs in Hong Kong

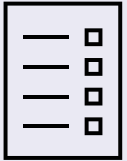
Enhancing AI Security from Within: A Practical Guide from PCPD

Ms Joanne WONG

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

11 September 2025

Why does AI Governance Matter to MNCs?



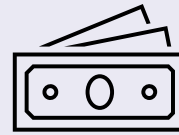
Compliance with laws and regulations on AI

- EU's **Artificial Intelligence Act**
- Mainland's
 - **National policies** (e.g. AI Safety Governance Framework)
 - **AI-specific regulations** (e.g. Measures for Labelling Artificial Intelligence-Generated Synthetic Content)



Compliance with existing legal frameworks

- Hong Kong's **Personal Data (Privacy) Ordinance (PDPO)** is a piece of principle-based, **technology-neutral** legislation



Financial loss and leakage of trade secrets

- Fraudsters may use AI technologies to orchestrate scams
- Unintended disclosure of trade secrets may occur when employees upload sensitive information to AI tools



Reputational harm

- A lack of transparency or the misuse of personal data can cause irreparable harm to an organisation's reputation

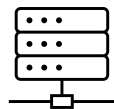
Local Context

According to the compliance checks conducted by PCPD in 2025,
among the 60 organisations examined:

48 organisations (80%) used AI in their day-to-day operations.
Among them:



42 organisations (around **88%**) had been using AI for
over a year



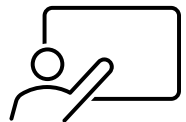
24 of them (**50%**) collected and/or used personal data
through AI systems

Local Context

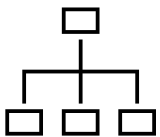
Among the 24 organisations that collected and/or used personal data through AI systems:



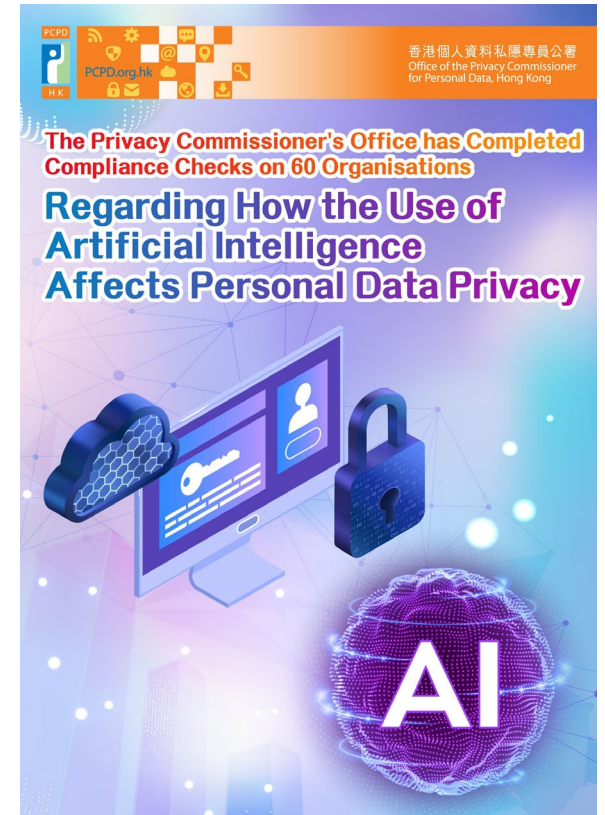
15 of them (about **63%**) formulated policies related to AI



18 of them (**75%**) provided training for employees regarding AI



19 of them (about **79%**) established AI governance structures



PCPD's Guidance

The PCPD has published different guidance in response to AI development

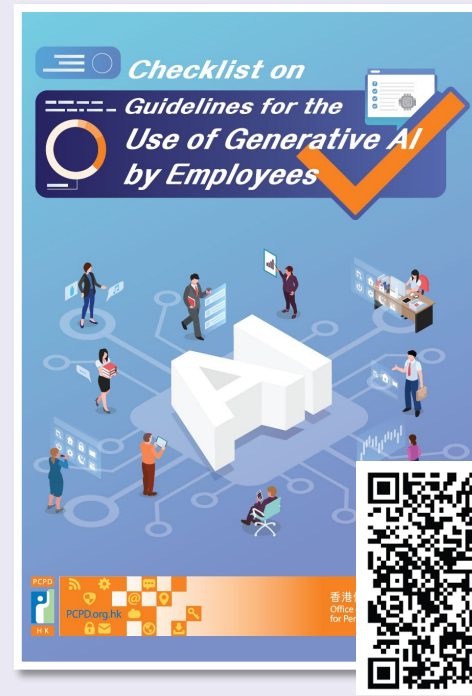
Organisations



Aug 2021



Jun 2024



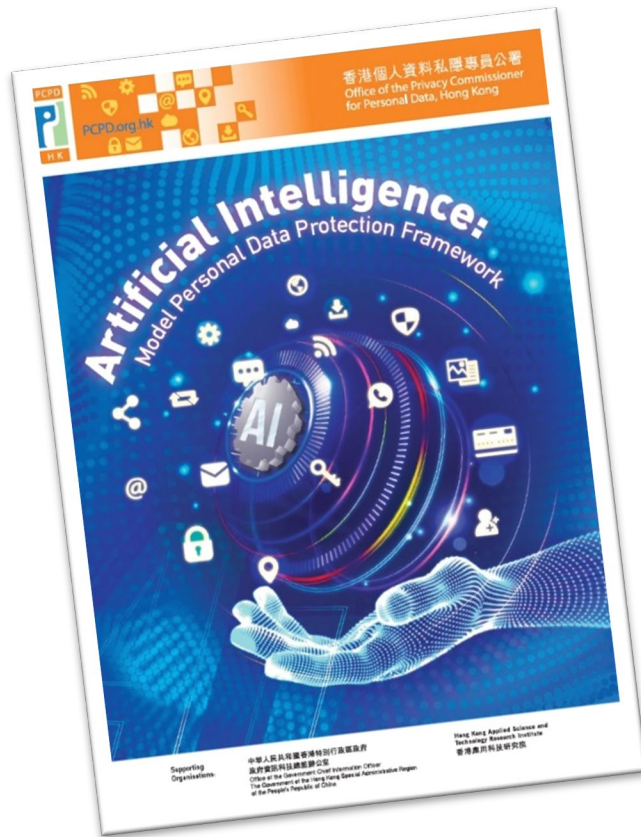
Mar 2025

Public

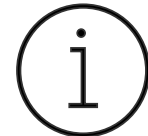


Sep 2023

Artificial Intelligence: Model Personal Data Protection Framework



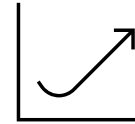
✓ Benefits



Assist organisations in complying with the requirements of the PDPO



Ensure AI Security

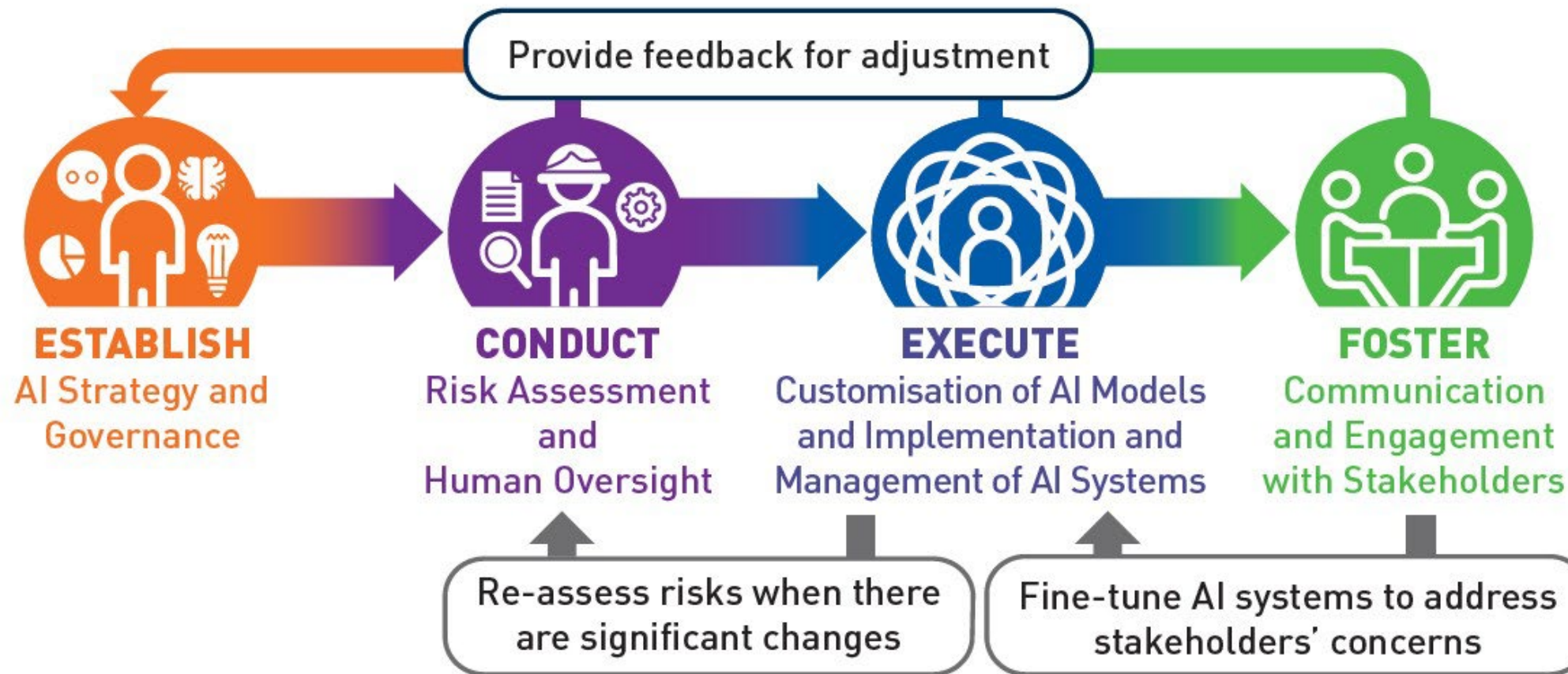


Increase competitiveness



Provide a set of recommendations on AI governance and the best practices for organisations procuring, implementing and using any type of AI systems, including generative AI (Gen AI), that involve the protection of personal data privacy

Model Personal Data Protection Framework



Formulate AI Strategy and Governance

9 governance considerations



Purpose(s) of using AI



Criteria and procedures
for reviewing AI
solutions



Plan for continuously
scrutinising changing
landscape



**Privacy and security
obligations and ethical
requirements**



Data processor
agreements



Plan for monitoring,
managing and
maintaining AI solution



International technical
and governance
standards



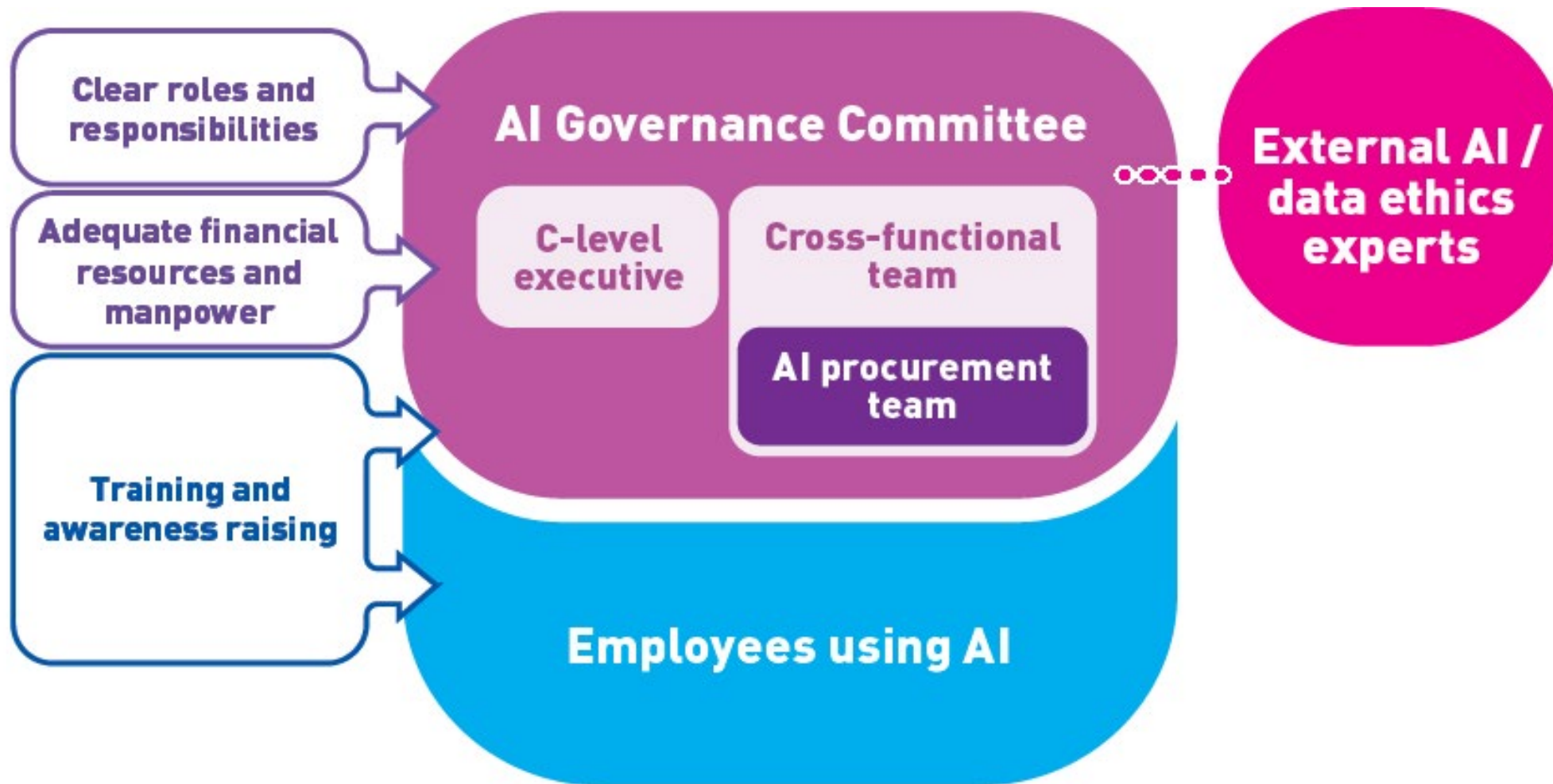
Policy on handling
output generated by
the AI system



Evaluation of AI
suppliers

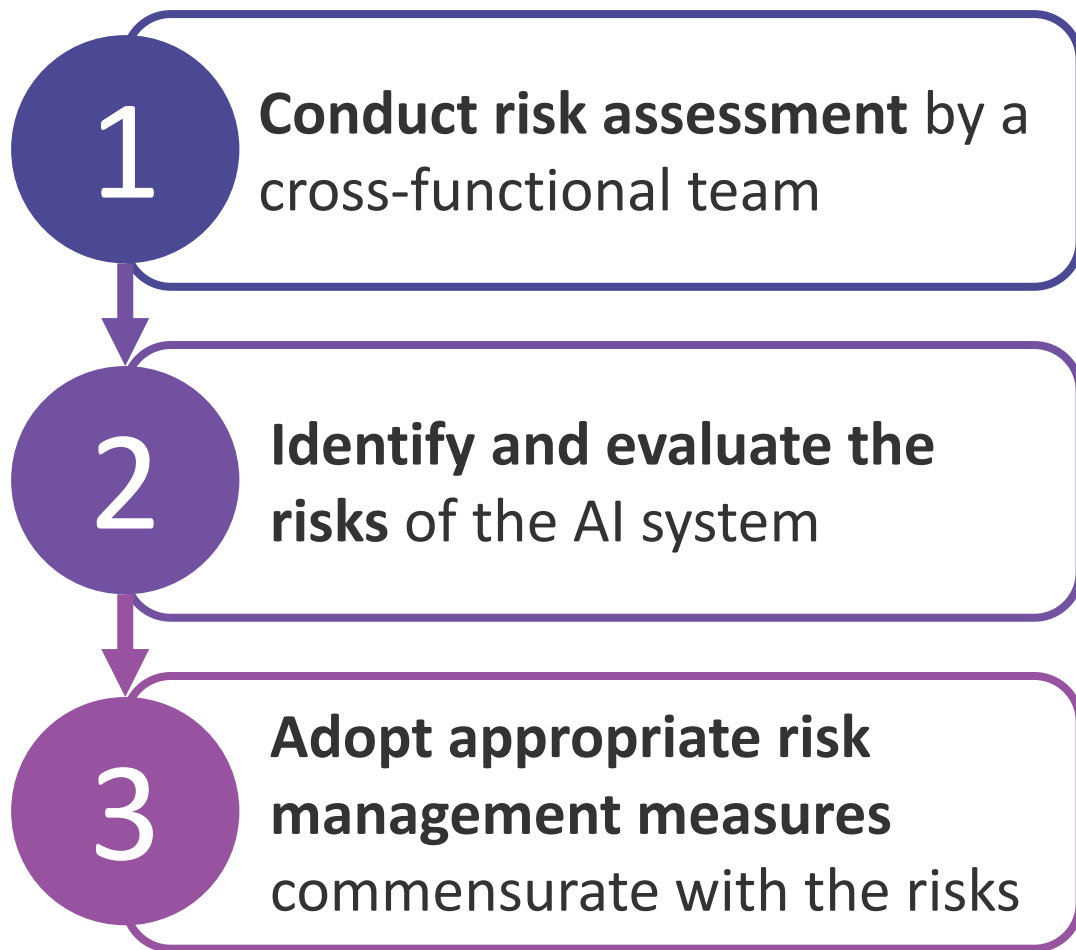
Formulate AI Strategy and Governance

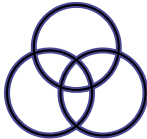

Governance structure



Conduct Risk Assessment and Human Oversight

Process of risk assessment



Risk type	Factors to be considered
Privacy risks 	<ul style="list-style-type: none">The allowable uses of the data for customising procured AI solutions and / or to be fed into AI systems to make decisionsVolume of personal dataSensitivity of data involvedThe security of personal data used in an AI system
Ethical risks 	<ul style="list-style-type: none">The potential impacts of the AI system on the affected individuals, the organisation and the wider communityThe probability that the impacts of the AI system on individuals will occur, as well as the severity and duration of the impacts

10

Conduct Risk Assessment and Human Oversight

Risk-based approach to human oversight



An AI system likely to produce an output that may have 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



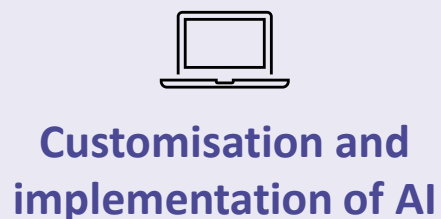
Human-in-the-loop

Human actors retain control in the decision-making process

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



Process



Recommendations



Ensure compliance with privacy law



Minimise the amount of personal data involved



Manage data quality



Document data handling



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



Maintain proper documentation



Establish an **AI Incident Response Plan**



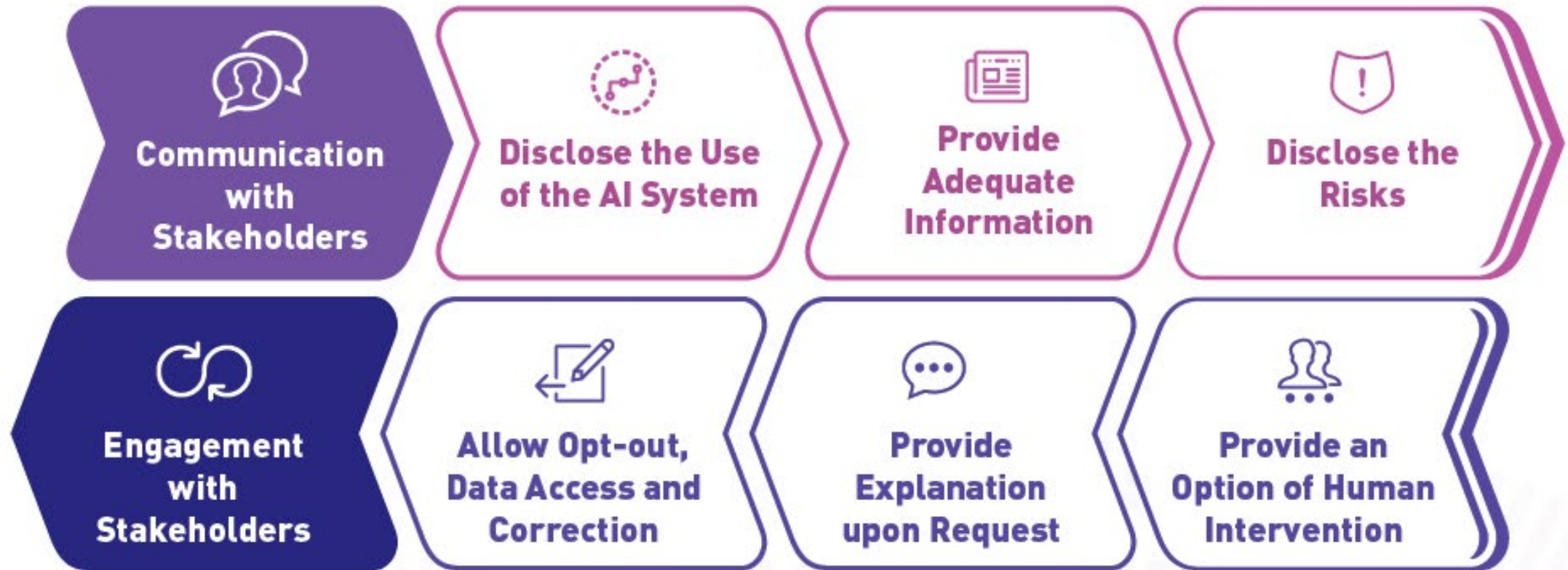
Conduct periodic audits



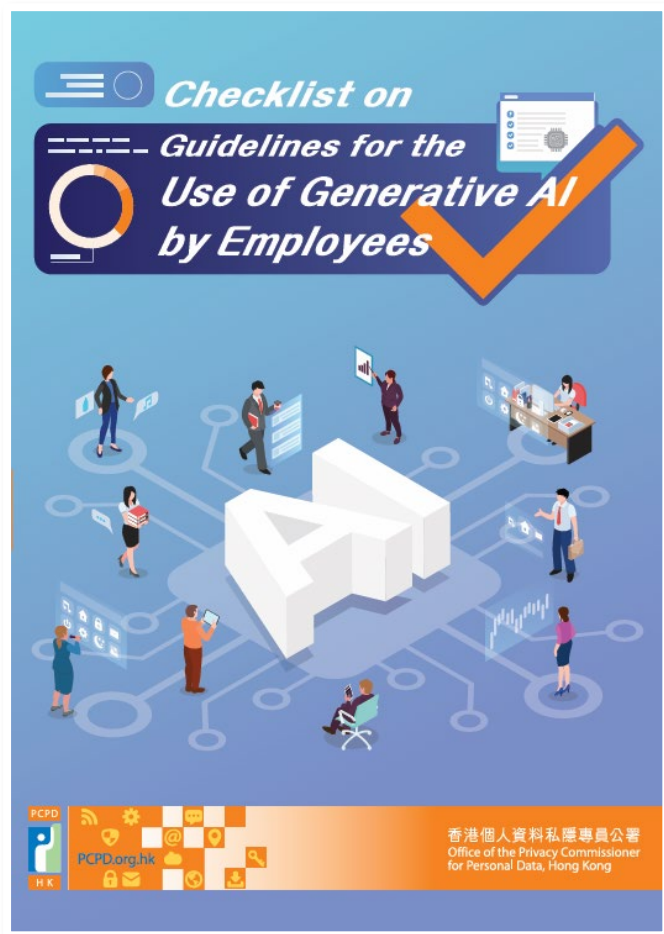
Consider incorporating review mechanisms as risk factors evolve

12

Foster Communication and Engagement with Stakeholders



Checklist on Guidelines for the Use of Generative AI by Employees



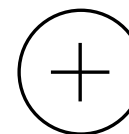
Objective

To assist organisations in developing internal policies or guidelines on the use of Gen AI by employees at work while complying with the requirements of the PDPO

Features

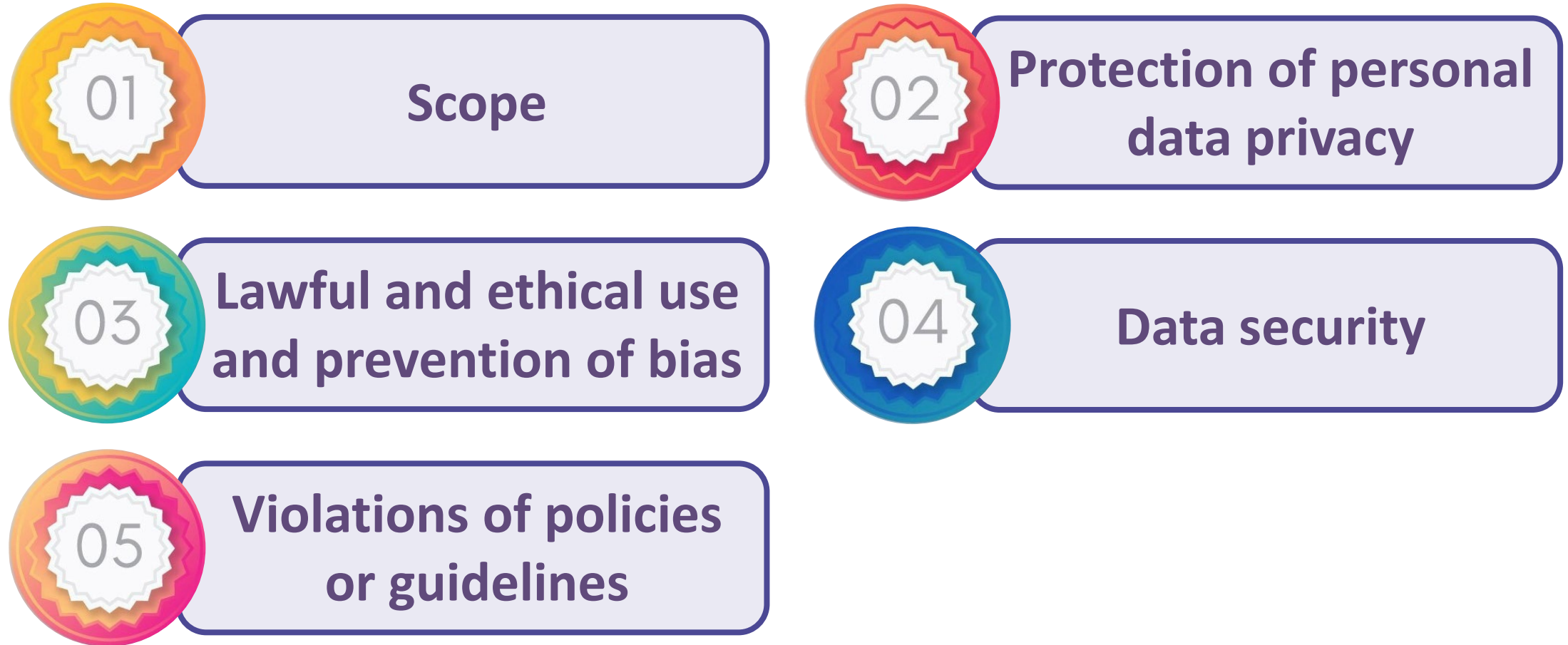


Presented in the form of a **checklist**



As a matter of good practice, organisations should devise their own policies and guidelines in alignment with their values and mission

Recommended Coverage



Enhance AI Security = Enhance Competitiveness



Download AI-related guidelines from the PCPD's webpage



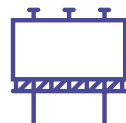
Evaluate organisation's strategies on the use of AI



Develop relevant governance strategies and framework, draft relevant internal policies or guidelines



For enquiries, please contact PCPD's "AI Security Hotline" (2110 1155)



Join PCPD's seminars and request internal training seminars

Thank you!



www.pcpd.org.hk



communications@pcpd.org.hk



Please
follow us!

