通訊事務管理局辦公室
OFFICE OF THE
COMMUNICATIONS AUTHORITY

TRAAC Paper No. 02/2026

Safeguarding Computer-system Security of Critical Infrastructures

Telecommunications Regulatory Affairs Advisory Committee
3 February 2026

An Overview of the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653)

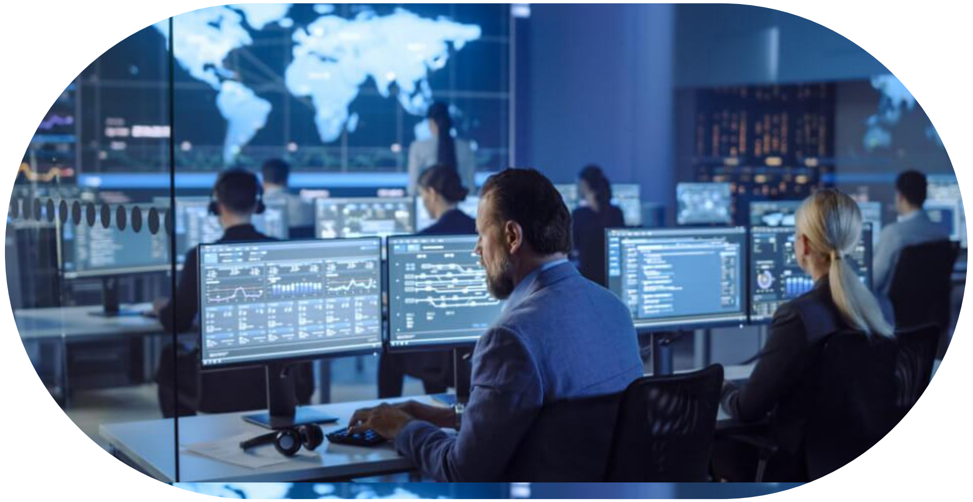
The Protection of Critical Infrastructures (Computer Systems) Ordinance ("PCICSO") comes into effect on 1 January 2026

- **Critical infrastructures** (CIs) refer to any infrastructure that is essential to the continuous provision in Hong Kong (HK) of an essential service in eight specific sectors, or any other infrastructure the damage, loss of functionality or data leakage of which may hinder or otherwise substantially affect the maintenance of critical societal or economic activities in HK

- Eight sectors specified under PCICSO

- Banking & Financial Services
- Telecommunications & Broadcasting Services
- Information Technology
- Land Transport
- Air Transport
- Maritime Transport
- Healthcare Services
- Energy

Purpose of the Ordinance



- To ensure the computer system security of CIs **necessary for the normal functioning of the HK society**

- To **minimise the chance of essential services being disrupted or compromised** due to cyberattacks, thereby enhancing the overall computer system security in HK

Targets of the Ordinance

Example

CIs in the Telecom and Broadcasting Services Sectors

↓

CI Operators

↓

Critical Computer Systems (CCS)

Telecom and Broadcasting Services Sector

- Essential to the core function of the CI
- Accessible by the CI operator in or from HK

Category 1 - Organizational Obligations

Maintain address and office in HK

Report changes in operator

Set up security management unit with dedicated supervisor

Purpose

Ensure sound management structure to implement necessary measures to protect CCSs

Category 2 - Preventive Obligations

- Report material changes to CCSs
- Formulate / implement security management plan
- Conduct regular security risk assessment
- Conduct regular independent security audit

Purpose

Ensure necessary measures in place to prevent cyberattacks

Category 3 - Incident Reporting & Response Obligations

Participate in security drill regularly

Prepare emergency response plan

Report security incident within specified time frame

Purpose

Ensure swift incident response and system restoration by CI operators

Act promptly to prevent further attacks, plug system vulnerabilities and stop the spread of attacks

Responsibilities of the Commissioner and CA

Commissioner of Critical Infrastructure (Computer-system Security) (“**Commissioner**”) **oversees the implementation** of the new regime, including enforcing Categories 1 & 2 obligations for those sectors under its purview and enforcing Category 3 obligations for all eight sectors specified in PCICSO

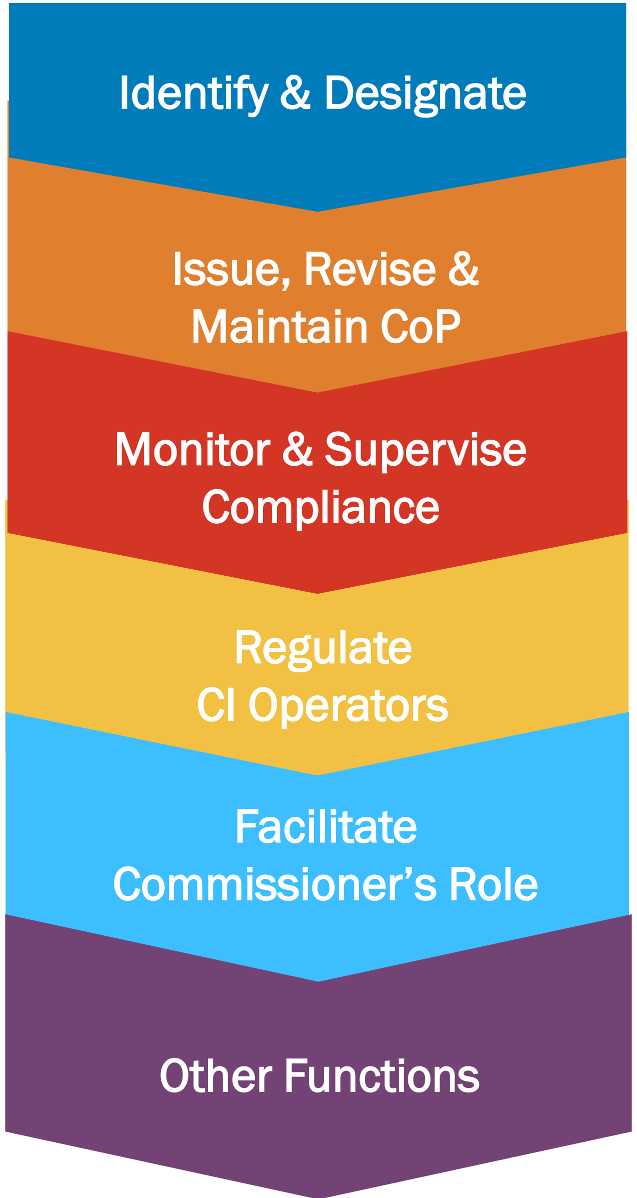
CA is the designated authority responsible for enforcing **Categories 1 & 2 obligations** in respect of the **telecommunications and broadcasting services sector**

	Designated Authority		Commissioner of Critical Infrastructure (Computer-system Security)
	Monetary Authority	Communications Authority	
Designation of CI operators/ Critical computer systems	Banking and financial services sector Operators currently regulated by the Monetary Authority	Telecommunications and broadcasting sector Operators currently regulated by the Communications Authority	Other operators
I. Organizational obligations			
II. Preventive obligations			
III. Incident reporting and response obligations	All operators		

Functions of CA under the PCICSO

As a designated authority, CA is responsible for:

- Identify CIs in telecom and broadcasting services sector
- Designate **CI operators** and their **CCSs**
- Monitor and supervise compliance with **Categories 1 & 2 obligations**
- Facilitate the Commissioner’s performance of functions under PCICSO


Identify & Designate
Issue, Revise & Maintain CoP
Monitor & Supervise Compliance
Regulate CI Operators
Facilitate Commissioner’s Role
Other Functions

- Issue, revise and maintain CoP for **Categories 1 & 2 obligations** of CI operators regulated by CA
- Issue directions, investigate offences in the event of operators’ failure to comply with **Categories 1 & 2 obligations**
- Perform any functions imposed or conferred on CA under the PCICSO

Telecommunications Operators Regulated by the PCICSO

CA may, by written notice, designate a regulated organization in the telecommunications services sector as a **CI operator** if the organization operates a CI specified by CA. Regulated telecommunications organizations include the following types of licensees –

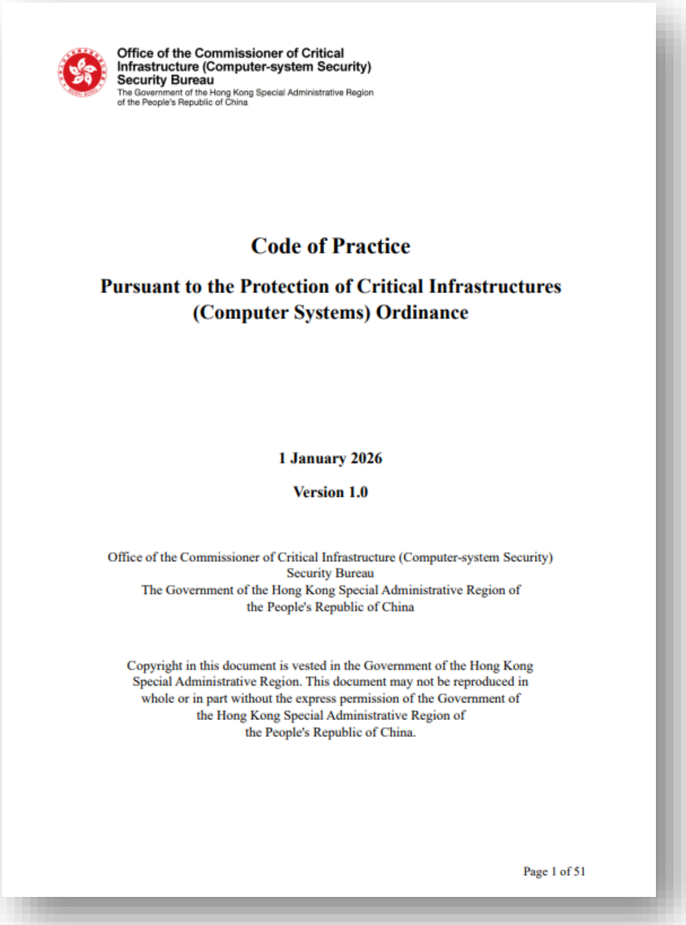
- A holder of a **unified carrier licence**; and
- A holder of a **space station carrier licence**

To prevent CIs in the telecommunications services sector from becoming targets of cyberattacks, CA **will not publish the list of CI operators designated** by CA.

Code of Practice (CoP)

- Commissioner's Office issued CoP to provide practical guidance in respect of the three types of obligations
- CoP (Generic) contains over 200 controls covering governance, risk management, protection, monitoring, incident response and disaster recovery
- Most of the controls can be mapped directly to internationally recognised standards such as ISO 27000 series, IEC 62443 and the NIST cybersecurity framework

CA adopts the CoP in respect of Categories 1 and 2 obligations of CI operators regulated by CA.



Office of the Commissioner of Critical
Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

Code of Practice

Pursuant to the Protection of Critical Infrastructures
(Computer Systems) Ordinance

1 January 2026

Version 1.0

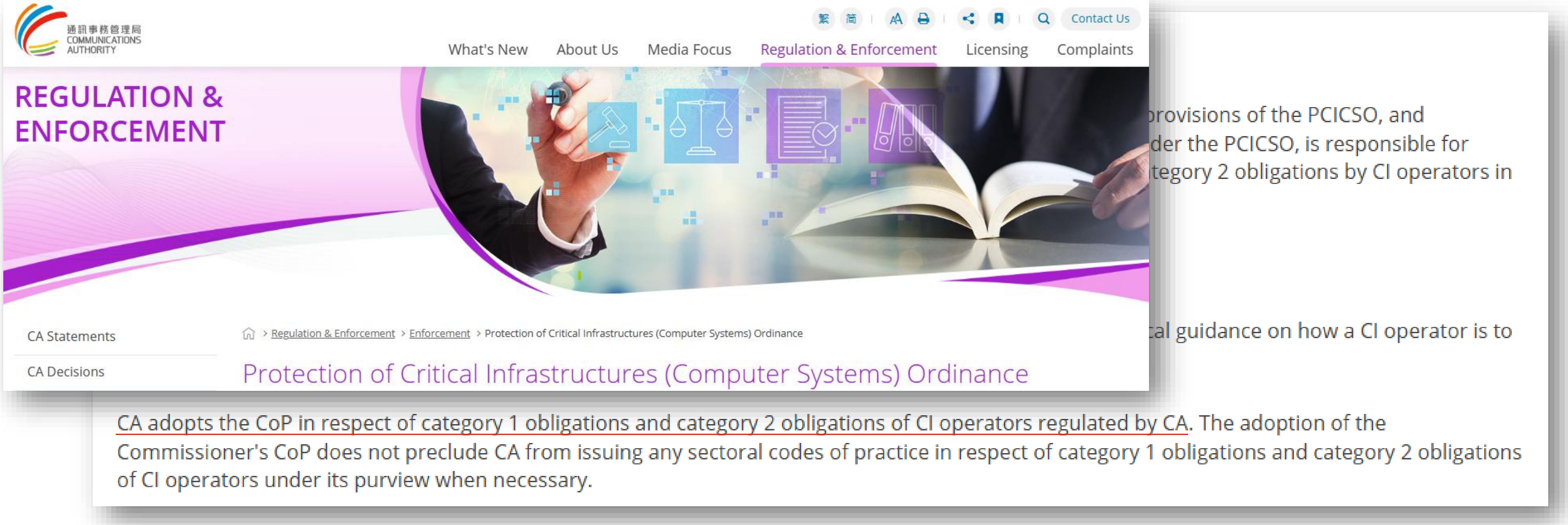
Office of the Commissioner of Critical Infrastructure (Computer-system Security)
Security Bureau
The Government of the Hong Kong Special Administrative Region of
the People's Republic of China

Copyright in this document is vested in the Government of the Hong Kong
Special Administrative Region. This document may not be reproduced in
whole or in part without the express permission of the Government of
the Hong Kong Special Administrative Region of
the People's Republic of China.

Page 1 of 51

Code of Practice (CoP)

CA's thematic website for PCICSO
(https://www.coms-auth.hk/en/policies_regulations/other/pcicso/index.html)



Regulation & Enforcement > Enforcement > Protection of Critical Infrastructures (Computer Systems) Ordinance

Protection of Critical Infrastructures (Computer Systems) Ordinance

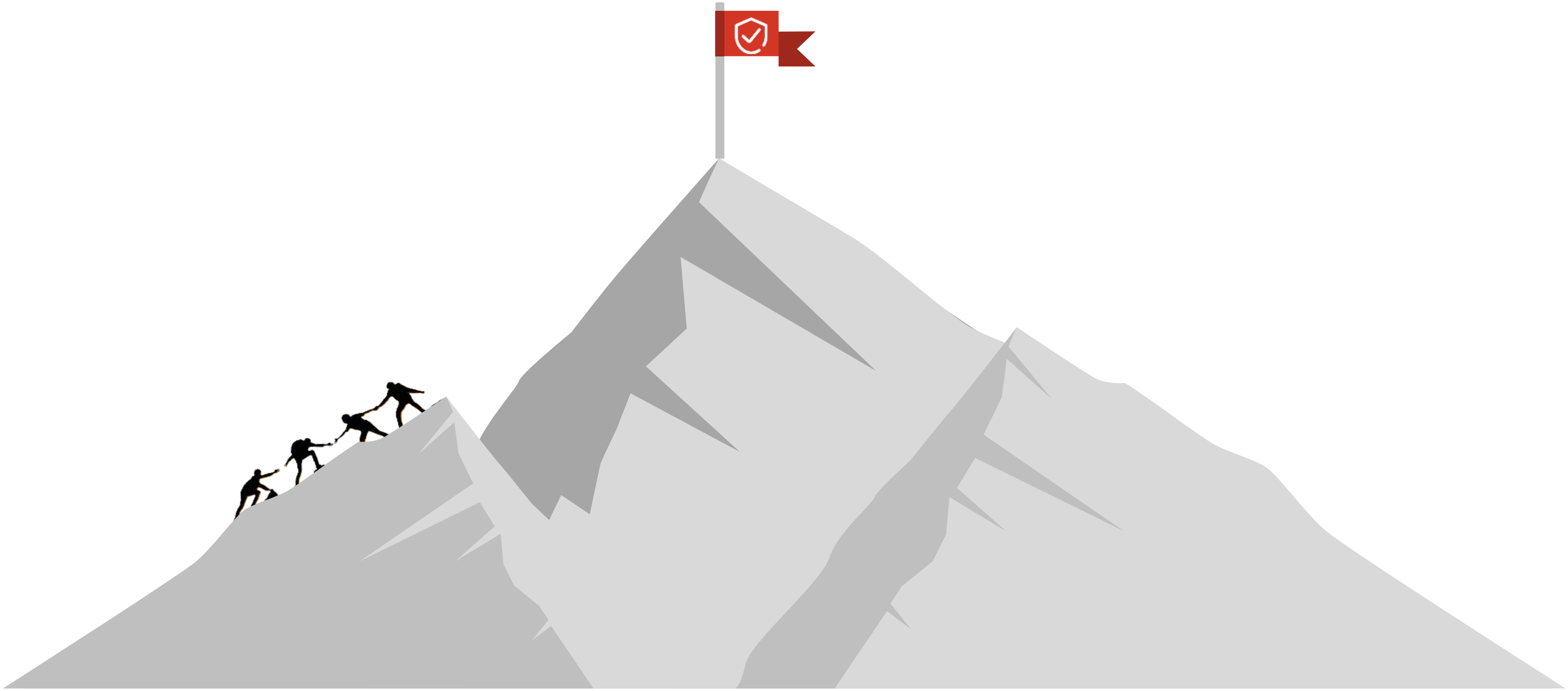
provisions of the PCICSO, and
der the PCICSO, is responsible for
tegory 2 obligations by CI operators in

al guidance on how a CI operator is to

CA adopts the CoP in respect of category 1 obligations and category 2 obligations of CI operators regulated by CA. The adoption of the Commissioner's CoP does not preclude CA from issuing any sectoral codes of practice in respect of category 1 obligations and category 2 obligations of CI operators under its purview when necessary.

Way Forward

We will partner with the Commissioner & CI operators in implementing the PCICSO effectively, with a shared mission of strengthening the security and resilience of the computer system security of critical telecommunications infrastructures.



THANK YOU