STEPHENSON HARWOOD
Wei Tu China Association
罗夏信-伟途 联营

September 2025

PROTECTION OF CRITICAL INFRASTRUCTURE (COMPUTER SYSTEMS) ORDINANCE

In recent years, laws and regulations protecting the security of computer systems of critical infrastructures ("**CIs**") have become increasingly common in many jurisdictions. Building on this momentum, on 19 March 2025, Hong Kong's Legislative Council passed the **Protection of Critical Infrastructures (Computer Systems) Bill**, marking a significant milestone in the region's cybersecurity regulatory framework. The **Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653)** (the "**Ordinance**"), which will take full effect on **1 January 2026**, aims to strengthen the security of the computer systems of CIs and minimise the chance of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall computer system security in Hong Kong.

TYPES OF CIS

Two types of CIs are covered in the Ordinance:

Type 1 CIs

Infrastructures essential to the uninterrupted delivery of essential services in Hong Kong across eight specified sectors:

- energy;
- information technology;
- banking and financial services;
- air transport;
- land transport;
- maritime transport;
- healthcare services; and
- telecommunications and broadcasting services.

Type 2 CIs

Other infrastructures for maintaining important societal and economic activities, such as major sports and performance venues, research and development parks.

ESTABLISHMENT OF REGULATORY GOVERNANCE STRUCTURE

The Security Bureau will establish a dedicated Commissioner's Office to oversee CI governance. This office will be led by a Commissioner of CI (the **"Commissioner"**), who will be appointed by the Chief Executive.

The key duties and functions of the Commissioner include, among other things, identifying CIs, designating CI operators ("**CIOs**") and Critical Computer Systems ("**CCSs**"), monitoring CI compliance, and regulating CIOs with regard to the computer system security of the CCSs.

The Commissioner may identify CIs and operate in conjunction with sector-specific Designated Authorities (**"DAs"**). The regulatory framework has initially appointed two primary DAs:

- the Hong Kong Monetary Authority, responsible for supervising the banking and financial services sector; and
- the Communications Authority, responsible for overseeing the communications and broadcasting sector.

The Commissioner and the DAs may designate an organisation operating a specified CI as a CIO.

Additionally, if a computer system that is accessible in or from Hong Kong is vital to the core operations of such an infrastructure, it may be classified as a CCS by the Commissioner and the DAs.

When making determinations about specified CIs, the Commissioner and the DAs must carefully evaluate multiple factors, including:

- the kind of service provided by the infrastructure;
- the implications if the infrastructure is damaged, loses functionality or suffers any data leakage; and
- any other matters the Commissioner or DAs consider relevant.

OBLIGATIONS OF CIOS

The Ordinance applies only to designated CIOs and their CCSs. These entities are subject to a comprehensive regulatory framework encompassing organisational, preventive, and incident response obligations, designed to ensure practical implementation of robust cybersecurity protections.

Category 1: Organisational Obligations

CIOs must:

- establish and maintain a registered office in Hong Kong;
- report operator changes in relation to the CIs; and
- maintain a computer system security management unit (which may be in-house or outsourced), supervised by an employee of the CIO who has professional knowledge.

Category 2: Preventive Obligations

CIOs must:

- inform the Commissioner's Office of material changes to their CCSs (such as design, configuration, security and operation);
- formulate and implement a computer system security management plan;
- conduct a computer system security risk assessment (at least once every year);
- conduct a computer system security audit (at least once every two years); and
- adopt measures to ensure that their third party service providers are in compliance with the relevant statutory obligations.

Category 3: Incident Reporting and Response Obligations

CIOs must:

- participate in a computer system security drill (at least once every two years);
- formulate an emergency response plan; and
- notify the Commissioner's Office of the occurrence of computer system security incidents in respect of CCSs.

What kinds of incidents do CIOs need to report?

CIOs will need to report computer system security incidents to the Commissioner's Office (i.e. activities carried out without lawful authority on or through a computer system that jeopardises or adversely affects its security) so that the Commissioner may instruct a timely response as needed.

Reporting Categories	Timeline
Serious computer system security incidents (incidents that have or are about to have a major impact on the continuity of essential services and normal operation of CIs, or that lead to a large-scale leakage of personal information and other data)	Report must be made within **2 *hours*** after becoming aware of the incident
Other computer system security incidents	Report must be made within **24 *hours*** after becoming aware of the incident

CONSEQUENCES FOR NON-COMPLIANCE

Potential Penalties

Any non-compliance will be subject to fines ranging from HK$500,000 to HK$5 million, plus daily fines for certain persistent violations, the maximum of which range from HK$50,000 to HK$100,000.

However, if the relevant violations involve a breach of existing criminal legislation, such as making false statements, using false instruments or other fraud-related offences, the officers involved may be held personally criminally responsible.

RECOMMENDED STEPS

What should organisations do next?

Step 1: Assess Potential CIO Status

Determine whether your organisation operates infrastructure that may be designated as a CIO under the Ordinance. This includes evaluating whether your services fall within the scope of Type 1 or Type 2 CIs, and whether your systems are integral to the continuity of essential services or societal functions.

Step 2: Consider Resources for Compliance

If your organisation is likely to qualify as a CIO, allocate appropriate resources to implement the necessary organisational changes.

Step 3: Analyse for Gaps

Conduct a comprehensive gap analysis by mapping your current cybersecurity practices against the requirements under the Ordinance.

Step 4: Implement Measures

Organisations should proactively implement measures to meet their obligations under the Ordinance. These may include:

- establishing clear incident reporting protocols in line with the 2-hour and 24-hour reporting thresholds;
- conducting regular drills and training sessions;
- developing or updating security management and emergency response plans; and
- reviewing and updating system architecture to ensure resilience.

By taking these steps, organisations can position themselves as leaders in regulatory readiness, while significantly reducing their exposure to cybersecurity risks and potential penalties. Early movers will gain a strategic advantage in navigating the evolving compliance landscape.

HOW WE CAN HELP

We offer comprehensive services to support every aspect of cyber incident preparedness. We assist clients in preparing for incidents and proactively managing cyber risks to ensure more efficient responses and minimise the impact of potential incidents.

Our team members have been working with other stakeholders on the formulation of the draft proposal to implement the cybersecurity regime. This positions us well to support and guide our clients in meeting the regulatory requirements for CI under the new legal framework.

Please get in touch if you are interested in discussing any of the above.

CONTACT US

DANNY KAN

Partner

+852 2533 2758
danny.kan
@stephensonharwood.com

ANGELA NG

Associate

+852 2533 2706
angela.ng
@stephensonharwood.com