Hong Kong's Protection of Critical Infrastructures (Computer Systems) Ordinance

FileCloud & Cloud Systems Asia Compliance Overview

> *"With the rapid development in information and communication technologies, the operation of critical infrastructures (CI) has become more dependent on the secure and smooth operation of computer systems, and at the same time faces increasing risks of cyberattacks."*
>
> - Legislative Council Panel on Security Consultation Report, 8 Oct 2025

Preparing for Compliance: File Sharing & Cloud Storage in Hong Kong

On January 1, 2026, the Protection of Critical Infrastructures (Computer Systems) Ordinance will go into effect in Hong Kong. In brief, this legislation serves to:

- Establish a regulatory body to set cybersecurity standards for Hong Kong's critical infrastructures.
- Identify industries that participate in or contribute to Hong Kong's critical infrastructures.
- Provide the regulatory body with organizational frameworks and enforcement mechanisms.

Legislative Timeline

March 19, 2025
The Hong Kong Legislative Council passes the Protection of Critical Infrastructures (Computer Systems) Bill ("the Bill"), establishing the legal basis for cybersecurity requirements.

March 28, 2025
The Legislative Council publishes the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance"). The Ordinance broadly organizes regulatory requirements, identifies impacted industries and regulatory authorities, and establishes penalties for compliance violations.

July 2 - August 1, 2025
Conclusion of the one-month consultation period, run by the Hong Kong Security Bureau.

October 8, 2025
The Legislative Council Panel on Security publishes the Consultation Report for the Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures.

January 1, 2026
The Ordinance goes into effect.

Impacted Industries

Critical Infrastructures (CIs): Any infrastructure that is essential to the continuous provision in Hong Kong of an essential service in the following sectors:

Energy

Land Transport

Air Transport

Maritime

Information Technology

Banking & Financial Services

Healthcare Services

Telecommunications & Broadcasting Services

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 Hong Kong (e.g. major sports and performance venues, research and development parks, etc.).

Regulatory Authority

Commissioner's Office & Designated Authorities

The Ordinance establishes the Commissioner's Office, which will operate under the Security Bureau. This office is responsible for coordinating cybersecurity efforts across CIs.

Designated Authorities will operate for certain sectors:

- Monetary Authority (for banking and financial services sector)
- Communications Authority (for telecommunications and broadcasting services sector)

Impacted Parties

Critical Infrastructure Operators (CIOs) & Critical Computer Systems (CCSs)

CIOs will be expressly identified by the Commissioner's Office as responsible for managing CI systems.

The Commissioner's Office will only identify computer systems as CCSs if they are considered relevant to the provision of essential services or core functions of CIs. Interruption or damage to these computer systems would seriously impact the normal functioning of the CIs.

Categories of Obligations

The Ordinance sets out three main categories of obligations for designated CIOs:

1. Organizational

   a. CIOs must establish an office in Hong Kong and notify the relevant Regulating Authority in writing of any change of operator

   b. CIOs are required to set up a dedicated unit to manage the security of computer systems and to follow up on directions given by the Commissioner's Office.

2. Preventive

   a. CIOs will conduct computer system security risk assessments and audits regularly, in accord with CoPs established by the Security Bureau.

   b. CIOs will report material changes concerning the design, configuration, security or operation of CCSs.

3. Incident Reporting and Response

   a. Organizations will conduct a timely investigation into the nature and cause of a serious computer system security incident within [2-12*] hours after becoming aware of the incident (or within [24-48*] hours after the occurrence of other incidents) and report to the Commissioner's Office, as required in the proposed legislation.

   b. CIOs will notify the Commissioner's Office within 24 hours after becoming aware of other computer system security incidents.

   c. CIOs will participate in computer system security drills organized by the Commissioner's Office, at least once every two years.

*subject to change based on Consultation Report

Enforcement

The Commissioner's Office will be established within one year of the Ordinance coming into effect; once established, enforcement by the Commissioner's Office will take place within half a year's time.

In the interim period, the Security Bureau and Commissioner's Office will communicate regularly with potential CIOs, and designation will take place in phases, relative to risk assessments, independent audits, and submission of relevant reports.

The Commissioner's Office will also develop Codes of Practice (CoP) to provide specific, detailed cybersecurity requirements that must be fulfilled by the CIOs. Time frames of enforcement will be tied directly with time of designation.

How to Prepare for Compliance

Companies in Hong Kong can begin preparing for the Protection of Critical Infrastructures (Computer Systems) Ordinance in a few simple steps:

1. **Check the list of industries identified by the Ordinance** to confirm if the organization might be categorized as a CIO or if systems might be categorized as a CCS.

2. **Remain alert to legislative updates on this Ordinance** published by the Hong Kong Legislative Council.

3. **Collaborate with the Security Bureau and the Commissioner's Office as it is being established;** contribute as necessary to early drafts of CoPs pertaining to your organization or industry.

4. **Allocate resources internally to support compliance, which may include:**

   a. setting up an office in Hong Kong

   b. creating a dedicated computer-system security management team or unit (if not already present)

   c. training employees in cybersecurity standards and providing specialized training to those involved in maintaining CCSs.

   d. developing cybersecurity incident and emergency response plans

   e. conducting security risk assessments, audits, and/or incident response drills

To support companies in Hong Kong, FileCloud and Cloud Systems Asia have created a proactive requirements checklist based on industry norms and similar cybersecurity regulations around the world.

Interested in exploring how a third-party cloud storage and file sharing solution can support compliance?

Check out the Requirements Checklist!