Protection of Critical Infrastructures (Computer Systems) Bill

An overview of the Bill and requirements stipulated

March 2025

Overview of the Bill

Hong Kong's Critical Infrastructure Bill aims to protect the computer systems of the designated Critical Infrastructure (CI's) in Hong Kong by establishing a regulatory framework to enhance cybersecurity and resilience against cyber threats.

The bill passed on 19 March 2025, will come into effect from 01 January 2026.

The bill imposes statutory requirements to ensure that operators of the designated Critical Infrastructure Organisations ("CIO's') deploy appropriate measures to protect their computer systems, strengthen their cybersecurity posture to minimise disruption to essential services and critical societal and economic activities as a result of cyber attacks.

Critical Infrastructure Providers

Designated Sectors: Organisations *vital for providing essential services* for day-to-day life. The organisations operating in the following eight sectors - **Energy, Information technology, Banking and Financial services, Land transport, Air transport, Maritime transport, Healthcare services and Telecommunications and Broadcasting services** are classified as "Designated Sector"

In addition, organisations *vital for maintaining critical societal and economic activities,* including Major sports and performance venues and Major Technology parks may also be considered as CI's

Key highlights

- The Bill stipulates strict guidelines on the cyber security obligations of the organisations operating Critical Infrastructure in Hong Kong.
- The Bill will be enforced by the Commissioner's Office under the Security Bureau and also designates regulators of certain industries as designated authorities including the Hong Kong Monetary Authority (to regulate the banking and financial services sector) and the Communications Authority
- Non-compliance with the obligations under the Bill may constitute offences punishable with maximum fines ranging from HK$500,000 to HK$5 million. If it is a continuing offence, the daily additional maximum fine ranges from HK$50,000 to HK$100,000 for each day the offence continues.
- The penalties under the Bill only apply to CIOs at the organisation level and do not extend to senior management at the individual level. However, if the violations involve criminal acts such as providing false information or fraud-related activities, then the relevant individuals may be held personally liable for those criminal acts.

Overview of the Key Obligations

Obligations	Summary of key obligations
Obligations relating to the organisation of CI Operators	• **Organisational Responsibilities to maintain an Office in Hong Kong**: CI operators must establish and maintain an office in Hong Kong to receive notices and other documents. • **Notify Changes in Operators**: CI operators are required to promptly notify regulatory authorities of any changes to the operator. • **Establish and Maintain a Computer System Security Management Unit**: CI operators must set up and continuously maintain a dedicated unit responsible for managing computer system security. Additionally, the CI operator must appoint an employee of the operator who has adequate professional knowledge in relation to computer-system security (adequate knowledge) to supervise the computer-system security management unit; and notify the Commissioner of this appointment in writing
Obligations relating to Prevention of Threats and Incidents	• **Report Significant Changes to Critical Computer Systems:** CI operators must notify regulatory authorities of significant changes to their critical computer systems. • **Submit and Implement a Computer System Security Management Plan:** CI operators must submit and implement a plan detailing measures to manage computer system security. The CI operator should *submit the plan within 3 months after operator's designation date unless extension is granted* • **Conduct Regular Risk Assessments:** CI operators are required to Conduct a computer-system security risk assessment *at least once every 12 months* and *submit a report within 3 months after each assessment period* (unless an extension is granted) • **Conduct an independent computer-system security audit** *at least once every 24 months and submit a report within 3 months* after each audit period (unless an extension is granted)
Obligations relating to Incident Reporting and Response	• **Participate in Security Exercises**: CI operators must participate in security exercises conducted by the Commissioner. • **Submit and Implement an Incident Response Plan**: CI operators must formulate and implement a plan to respond to incidents within 3 months after receiving designation as CIO (unless an extension is granted) • **Report Computer System Security Incidents**: CI operators are obligated to report incidents to the Commissioner within the specified timeframe.

Source: The Government of the Hong Kong Special Administrative Region Gazette

In simplified terms, a cyber security incident involving a critical computer system is any unauthorised or unlawful access or action that harms its security, whether done directly or through another computer system.

Key actions for Critical Infrastructure Organisations

Know your current state

Conduct reviews and security assessments with an aim to identify your current state of threat detection capabilities. This may include activities such as red team/ purple team and conducting incident response trainings for the Security Operations Teams aligned with your technology and tools environment to reduce the learning curve.

Cyber Incident Response Plan and Playbooks

Prepare, review and revise your cyber incident response plan to incorporate holistic and accurate determination of cyber incident classification and severity. While operational technology is not separately defined and might be considered part of core operations, we recommend reviewing the incident readiness of your OT threat detection capabilities.

Know your Regulatory obligations

The Bill defines Commissioner within the Security Bureau is tasked with implementation of the Bill however, the bill also recognises specific sector regulators such as the Hong Kong Monitory Authority, Communications Department as "Designated Authorities" and empowers them to issue codes of practice, use them in legal proceedings, and specify formats for compliance-related documentation.

Build Muscle Memory- Cyber Crisis Exercises and Drills

Perform Cyber Drills to practice and establish individual roles of the crisis management team within the organisation and identify gaps and actionable items to mitigate gaps and strengthen the incidence response efforts

Comprehensive cyber risk evaluations and security reviews

Conduct thorough risk analyses of your organisation to identify vulnerabilities and threats that could disrupt core operations, stemming from geopolitical challenges, third-party dependencies, cloud environments, and operational technologies.

How we can help ?

Protect

Cyber Crisis Simulation Drills and wargames

- Tailored exercises that mimic real world incidents with injects as challenges faced by organisation during incidents to strengthen decision making process, build understanding of individual roles and mitigate process gaps

Incident response plan and playbook development

- Assistance in creation of an incident response program aligned with organisations risk framework including tailored cyber playbooks for enabling rapid response

Cyber security risks assessments & Security testing

- Assist organisation in security testing such as vulnerability management & penetration testing

Bespoke Trainings for Security Operations Team

- Conduct technical trainings for security operations teams to boost incident detection and response

Detect

Proactive Threat Identification and Monitoring

- Continuous monitoring checks and early warnings driven by cyber threat intelligence approach to boost threat detection and proactive reviews.
- Tailored Threat Hunting driven reviews to identify malicious/ unauthorized activity within environment

Red/ Blue/ Purple Team Exercise

- Assist security teams in testing defense against common threat, tactics, procedures (TTP's) and help in identifying gaps, integrate new data sources and increase visibility for strengthening detections and reducing noise

Improving Threat Detection

- Assist security teams in developing tailored detection rules, integrations and automating threat identification and mitigation capabilities

Investigate

Cyber Incident Response

- On-demand assistance in resolving cyber incidents end-to-end which includes all phases of incident response process, viz. digital forensic triage, containment, investigation, remediation, recovery and reporting.

Digital Forensic Investigations

- Assistance with conducting digital forensic fact finding investigations to forensically preserve and review evidence from IT, OT and Cloud systems

Independent verification and validation

- The verification of investigation findings and extent of cyber security breach as an independent expert. KPMG's tested track record of independence can help ensure the accuracy and completeness of any investigation.

Contact us

Chad Olsen
Partner and Head of Forensics-Hong Kong
Hong Kong
KPMG China
chad.olsen@kpmg.com

Brian Cheung
Partner
Technology Consulting
Hong Kong
KPMG China
brian.cheung@kpmg.com

Mohit Kumar
Director, Cyber Incident Management
Hong Kong
KPMG China
mohit.kumar@kpmg.com

About KPMG

KPMG in China has offices located in 31 cities with over 14,000 partners and staff, in Beijing, Changchun, Changsha, Chengdu, Chongqing, Dalian, Dongguan, Foshan, Fuzhou, Guangzhou, Haikou, Hangzhou, Hefei, Jinan, Nanjing, Nantong, Ningbo, Qingdao, Shanghai, Shenyang, Shenzhen, Suzhou, Taiyuan, Tianjin, Wuhan, Wuxi, Xiamen, Xi'an, Zhengzhou, Hong Kong SAR and Macau SAR. It started operations in Hong Kong in 1945. In 1992, KPMG became the first international accounting network to be granted a joint venture licence in the Chinese Mainland. In 2012, KPMG became the first among the "Big Four" in the Chinese Mainland to convert from a joint venture to a special general partnership.

KPMG is a global organisation of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organisation or to one or more member firms collectively.

KPMG firms operate in 142 countries and territories with more than 275,000 partners and employees working in member firms around the world. Each KPMG firm is a legally distinct and separate entity and describes itself as such. Each KPMG member firm is responsible for its own obligations and liabilities.

Celebrating 80 years in Hong Kong

In 2025, KPMG marks "80 Years of Trust" in Hong Kong. Established in 1945, we were the first international accounting firm to set up operations in the city. Over the past eight decades, we've woven ourselves into the fabric of Hong Kong, working closely with the government, regulators, and the business community to help establish Hong Kong as one of the world's leading business and financial centres. This close collaboration has enabled us to build lasting trust with our clients and the local community – a core value celebrated in our anniversary theme: "80 Years of Trust".

kpmg.com/cn/socialmedia