Baker McKenzie.

Client Alert

January 2025

Hong Kong: The first draft of the new critical infrastructures cybersecurity law is here

In brief

The Hong Kong Government has published on 6 December 2024 a draft of the Protection of Critical Infrastructures (Computer Systems) Bill ("**Bill**"), marking a significant step towards enhancing cybersecurity standards in relation to essential services and critical societal or economic activities in Hong Kong. This Bill aims to protect the security of the critical computer systems (CCSs) of critical infrastructures (CIs), to regulate operators of CIs (i.e., critical infrastructure operators (CIOs)) and to provide for the investigation into, and response to, computer-system security threats and incidents. This article considers the key provisions of the Bill, compares the differences between the original legislative proposal and the Bill, and discusses areas of uncertainty with some key takeaways as things stand now. With significant obligations and penalties (from HKD 300,000 up to HKD 5 million plus daily penalty for a continuing offence), potential CIOs and service providers should watch this space closely for further developments and undertake suitable preparatory work, such as assessing the likelihood of designation, readiness of its existing cybersecurity framework and organizational structure for compliance and contractual provisions for risk allocation and mitigation.

Contents

Key takeaways

The draft provides much-needed clarity on various aspects of the legislative framework, particularly regarding the process of designation of CIOs and CSSs, as well as compliance standards. Organizations are recommended to conduct self-assessments to determine the likelihood of being designated by the Regulating Authorities. We are able to assist with assessments of the likelihood of an individual infrastructure or operator being regarded as a CI or a CIO, respectively.

For organizations with a higher likelihood of being designated, it is advisable to consider their existing cybersecurity framework in order to ensure compliance with the three categories of obligations, and to start formulating the required CCS management plans and/or emergency response plans in accordance with the requirements outlined in Schedule 3 of the Bill. This is especially important for multi-nationals facing competing obligations under different legal regimes (e.g., the EU's NIS2 Directive) and organizations subject to additional sector-specific regulations. We are able to assist with drafting such plans and revising them once the COPs are available.

Potential CIOs and customers that rely on CIs should review existing supplier contracts in light of the Bill to ensure sufficient protection, especially for provisions relating to compensation, audit rights, service levels and termination. Third party service providers (e.g., cloud providers) may expect that their CIO customers would attempt to flow down certain obligations under the Bill, given the liability of CIOs in relation to CIs.

Particularly for companies with interconnected computer systems located outside of Hong Kong, it is important to consider whether computer system accessibility limitations need to be imposed, as much of the Bill's obligations depend on accessibility rather than geographical location or control.

In more detail

For more background of the proposed legislation, please refer to our previous client alerts: July client alert and December client alert.

1. Key components of the Bill

The key operative provisions of the Bill are set out in Part 2 (Regulating Authorities), Part 3 (Critical Infrastructures, CI Operators and Critical Computer Systems), Part 4 (Obligations of CI Operators) and Part 5 (Responding to Computer-system Security Threats and Computer-system Security Incidents). The content of the Bill is largely similar to the Government's proposal outlined in the brief to the Legislative Council (LegCo) and the subsequent Consultation Report, as set out in our previous client alerts mentioned above, with a few key differences, namely:

- The term "interconnected" has been deleted from the factors for consideration in designating a CCS.
- Incident reporting and response timeframes have been relaxed, from 2 hours to 12 hours for a CCS security incident that has disrupted, is disrupting or is likely to disrupt the core function of the CI and from 24 hours to 48 hours in other cases.
- The defences of "due diligence" and "reasonable excuse" to a breach of the obligations under the Bill, available in certain circumstances, have been set out in more detail.

The key components of the Bill have been set out below:

- **CIs:** Defined in the same as was previously proposed, i.e., any infrastructure that is essential to the continuous provision in Hong Kong of an essential service in a specified sector (i.e., energy, information technology, banking and financial services, air transport, land transport, maritime transport, health services, and telecommunications and broadcasting services) and 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).
- **Commissioner:** The Chief Executive will appoint a new Commissioner of Computer-system Security ("**Commissioner**"), who, along with designated authorities for specific sectors ("**Designated Authorities**"), will serve as the regulating authorities (together, "**Regulating Authorities**"). Their key responsibilities include identifying and/or designating CIs, CIOs and CCSs, issuing Codes of Practice (COPs) and monitoring, investigating and responding to CCS security threats and incidents, all as further discussed below. A breach of the COPs will not by itself attract any civil or criminal liabilities, but such breach may be admissible in legal proceedings as evidence in relation to an alleged breach of the provisions of the Bill.
- **Designated Authorities for specific sectors**: The Monetary Authority and the Communications Authority are nominated as the Designated Authorities for regulated organizations in the banking and financial services sector and the telecommunications and broadcasting services sector, respectively, who will be given similar powers and duties as the Commissioner in relation to their specific sectors in monitoring the CIOs' discharge of their category 1 and 2 obligations (see below), although the Commissioner has sole power in relation to category 3 obligations. The Secretary for Security may by notice designate more sector-specific regulators in the future.
- **Regulatory powers**: The Regulating Authorities may give directions to CIOs directing them to do or refrain from doing any act in order to comply with the CIOs' obligations ("**Compliance Directions**"), in addition to publishing COPs. The Regulating Authorities may also request information from CIOs to better understand CCSs and to ascertain compliance with category 1-3 obligations (see below).
- **Designation of CIs and CCSs**: The Regulating Authorities may ascertain whether an infrastructure is a CI and designate individual CIOs and CCSs after taking into account a range of factors, and are given the power to request information from an organization that operates or has control over, or appears to be operating or have control over, an infrastructure. A system, whether under the control of the CIO or not, may be designated as a CCS if it is accessible by the CIO in or from Hong Kong and is essential to the core function of a CI operated by the CIO.
- **CIOs' obligations:**

  Category 1 (organizational) obligations:[1]

  (i) Maintain an office in Hong Kong and notify the Regulating Authority of any change of the correspondence address.

[1] Notifications of any changes must be made within one month.

© 2025 Baker & McKenzie | 2

(ii) Notify the Regulating Authority of a change of the organization that operates the CI.

(iii) Set up and maintain a CCS security management unit, either internally or through a service provider, and notify the Regulating Authority of the appointment and change of the supervising employee.

Category 2 (preventive) obligations:[2]

(i) Notify the Regulating Authority of specified changes as set out in Section 22 of the Bill[3] in respect of a CI operated by the CIO.

(ii) Submit to the Regulating Authorities and implement a CCS security management plan within three months of the CIO being designated.

(iii) Conduct and submit a report on an annual CCS security risk assessment.

(iv) Conduct and submit a report on a bi-annual CCS security audit by an independent auditor.

Category 3 (incident reporting and response) obligations:

(i) Participate in a CCS security drill conducted by the Commissioner on written notice by the Commissioner.

(ii) Submit to the Commissioner and implement a CCS security incident emergency response plan within three months of the CIO being designated.

Notify the Commissioner of any CCS security incident and submit a further written record and/or report of the incident in the specified form and manner within the specified time limits under Schedule 6 of the Bill (i.e., 12 hours after becoming aware in the case of incidents disrupting or likely to disrupt the core function of the CI and 48 hours in any other case).

- **Commissioner's powers to respond to CCS security threats/incidents**: The Bill grants the Commissioner the authority to conduct inquiries and investigations into CCS security threats/incidents through the following measures, listed in order of increasing intrusiveness:

(i) Direct an authorized officer of the Commissioner ("**Authorized Officer**") to make inquiries with the investigated CIO to identify the CCS security threats/incident, or carry out an investigation into and to respond to the threat/incident, during which the Authorized Officer will be given the power to request the investigated CIO to produce documents (defined broadly to include any input or output, in whatever form, into or from an information system, and any document, record of information or similar material (whether produced or stored mechanically, electronically, magnetically, optically, manually or by any other means)), give an explanation or further particulars in relation to the documents, and provide oral or written answers to questions.

(ii) Apply for a Magistrate's warrant authorizing an Authorized Officer, both for early intervention and for CCS security investigations purposes, to enter any premises to search for, inspect, make copies of, take extracts from, seize and remove any relevant documents on the premises.

(iii) Require the investigated CIO to do specified acts (e.g., perform a scan of the investigated CCS, carry out remedial measures, give the Authorized Officer all reasonable assistance in connection with the investigation and refrain from using the investigated CCS).

(iv) Apply for a Magistrate's warrant to impose requirements on an organization other than the investigated CIO that has or appears to have control over the investigated CCS ("**Other Organization**") (e.g., produce any documents in its possession, under its control, or otherwise accessible by it in or from Hong Kong, answer questions, give the Authorized Officer all reasonable assistance and refrain from using the investigated CCS).

---

[2] The deadline for submitting plans and reports is three months and for notifying any changes is one month.

[3] Namely: (i) a material change to the design, configuration, security or operation of a CCS of the CI; (ii) a CCS of the CI is removed; (iii) a computer system that is eligible to be designated as a CCS is added to the CI; and (iv) an existing computer system of the CI becomes eligible to be designated as a CCS.

© 2025 Baker & McKenzie | 3

(v) Apply for a Magistrate's warrant to access, inspect and carry out remedial measures in relation to the investigated CCS or another computer system that is accessible via the investigated CCS and is likely to be relevant to the investigation ("**Accessible System**").

(vi) Authorize an Authorized Officer to exercise some of the powers set out above (e.g. to search for and make copies of documents in the investigated system or an Accessible System and carry out remedial measures) in emergencies where it is not reasonably practicable to obtain a warrant.

- **Appeal mechanism**: The Bill establishes an appeal mechanism against several types of decisions (e.g., designation of CIOs or CCSs, and giving Compliance Directions). The decision of the appeal board is said to be final. The Bill does not otherwise have an express provision stating that a decision of the appeal board or the Regulating Authorities cannot be challenged by judicial review.
- **Exemption**: The Commissioner may exempt a CIO from any of the category 1-3 obligations, after taking into account whether the CIO has done, or is doing, an act that can achieve the same purpose as the compliance with the subject obligation and whether the CIO is subject to any alternative obligation that corresponds substantially to the subject obligation.
- **Due diligence and reasonable excuse defences:** In any legal proceedings for an offence of non-compliance with the Compliance Directions or the category 1-3 obligations, the defendant can rely on a due diligence defence if the commission of the offence was due to a cause beyond its control and it took all reasonable precautions and exercised all due diligence to avoid the commission of the offence. The onus is on the defendant to adduce evidence to support such defence. The defence of reasonable excuse is available in relation to certain offences.

2. Key areas of uncertainty or concern

- **Regulating Authorities' unrestricted powers to request information from potential CIOs**: The power of Regulating Authorities to request information from any organization that appears to be operating or have control over a CI is only limited by the requirement of reasonable necessity. There is no limitation, for example, on the scope of information to be requested (e.g., where disclosure is prohibited by foreign law), no clarity as to what the reasonable excuse defence would cover (in contrast to the provisions concerning security incident investigations, which require the relevant documents to be accessible in or from Hong Kong), and no territorial or geographical limitation on the organizations that may be subject to such requests. Such requests for information are not within the scope of the statutory appeal mechanism, implying that the only recourse an organization may have is potentially judicial review, which is only available with leave of the Court of First Instance of the High Court.
- **Territorial limitations**: In the Consultation Report, the Government reassured the public that the Bill will not have extraterritorial effect. Aside from the above power to request information from potential CIOs, the parts of the Bill that appear to delineate its territorial scope may be interpreted in an expansive manner, for example:

  (i) There is no requirement that a CCS (including its physical servers) must be physically located in Hong Kong, and the only territorial requirement is that the system is accessible by the CIO in or from Hong Kong, regardless of whether the CIO has control over it.

  (ii) In an inquiry or investigation on a CCS security threat/incident, the Commissioner's power to request a CIO to produce documents extends to those accessible in or from Hong Kong by the CIO, as long as they are relevant, or likely to be relevant, to the inquiry and/or investigation, and an Authorized Officer may, subject to obtaining a Magistrate's warrant, access and inspect, and carry out any remedial measures in relation to, as well as search for and make copies of information that is stored in an Accessible System.

  (iii) There is no limit to the geographical location of the Other Organization that could be subject to a Magistrate's warrant to provide assistance in connection with an investigation (although there would be practical limitations on the enforceability of such warrant against an organization located in a foreign jurisdiction).

  Given that some CIOs will likely be multi-national corporations, the territorial scope being determined by accessibility, instead of the more onerous threshold of geographical location or control, would imply that computer systems operated by their foreign affiliates within the same corporate group could nevertheless be subject to the disclosure requirements. Given that overseas jurisdictions may likewise have their own cybersecurity and/or data localization requirements, some multi-national corporations may wish to impose internal ring-fencing solutions to prevent its overseas computer systems from being subject to the disclosure requirements under the Bill.

© 2025 Baker & McKenzie | 4

- **Uncertainty in the obligation to notify operator changes**: In the Consultation Report, in response to the public's concerns over the difficulty for listed companies to report to the Commissioner of changes in ownership of CIs, the Government stated that it would seriously consider removing such requirements. However, the obligation to report an "operator change" (defined as a change of the organization that operates the CI) remains in the Bill. The lack of clear definition leaves uncertainty as to its scope, as various scenarios with differing degrees of change could be considered a "change", for example, a (full or partial) transfer of ownership of the CI (or the assets or facilities involved), a change in shareholdings of the CIO, which may or may not result in a change of control, or where another party, via contractual means, gains access to and/or control over a CI.
- **Powers over an Accessible System**: Accessible System is defined very broadly in the Bill to include any computer system accessible via the investigated CCS. To the extent that another computer system is located outside of Hong Kong but is accessible via the investigated CCS (which may itself be a CCS located outside of Hong Kong), it would appear that the Commissioner has the power to request information from such Accessible System provided that the Commissioner has obtained a Magistrate's warrant permitting it to do so. Given the interconnected nature of modern computer systems, many of which are linked via the internet and can be remotely accessed, this expansive definition could potentially encompass a vast array of systems beyond the investigated CCS.
- **Self-incrimination**: There are various provisions in the Bill which require an organization or its representative to answer the inquiries of or provide documents to an Authorized Officer. Self-incrimination cannot be used as an excuse to refuse compliance. While the Bill provides that self-incriminating answers are not admissible in certain criminal proceedings, some may consider this protection to be inadequate because the person has to claim the privilege against self-incrimination before answering, and the non-admissibility of self-incriminating answers is not applicable to criminal proceedings relating to an offence of non-compliance with the Commissioner's inquisitorial and investigatory powers, or a perjury offence.

It is hoped that these uncertainties will be addressed in subsequent drafts of the Bill, the implementing regulations and CoPs.

3. What to expect next?

The Bill was introduced into the LegCo on 11 December 2024, with the Second Reading debate being adjourned. A Bills Committee has been formed and its first meeting will be held on 7 January 2025, where LegCo members will evaluate the general merits, detailed provisions, and potential amendments to the Bill.

Potential CIOs and service providers should watch this space for further developments. Given the Bill's significant public interest, it is standard practice for the Bills Committee to invite views from the public in a window of two to three weeks. We are able to assist with formulating comments for submissions during this period.

* * * * *

Jacqueline Wong, Knowledge Lawyer, has contributed to this legal update.

© 2025 Baker & McKenzie | 5

Contact Us

Isabella F. C. Liu
Partner
isabella.liu@bakermckenzie.com

Dominic Edmondson
Special Counsel
dominic.edmondson@bakermckenzie.com

© 2025 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.