Volume 3, Number 4 July–August 2026

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 3, No. 4 July–August 2026

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL (ISSN 2995-7486) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: David Nayer
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

The photo on this journal's cover is by Gaël Gaborel—A Picture of the Earth on a Wall—on Unsplash

Cite this publication as:

The Global Regulatory Developments Journal (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

David Nayer, Publisher, Full Court Press at david.nayer@clio.com or at 202.999.4777

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2995-7486

Hong Kong Issues Code of Practice Under the Protection of Critical Infrastructures (Computer Systems) Ordinance

Gabriela Kennedy and Joanna K.C. Wong*

In this article, the authors discuss a new Code of Practice that clarifies key requirements under the Hong Kong new critical infrastructure cybersecurity regime and sets a baseline for compliance across sectors.

The Office of the Commissioner of Critical Infrastructure of Hong Kong has issued a Code of Practice (the CoP) under the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) (the Ordinance), which came into force on the same day. The CoP clarifies key requirements under the Hong Kong new critical infrastructure cybersecurity regime and sets a baseline for compliance across sectors.

On the same date, the Hong Kong government appointed Francis Chan Wing-on, former Chief Superintendent of the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force, as Commissioner of Critical Infrastructure for a three-year term.

The CoP translates the high-level obligations under the Ordinance into specific, actionable requirements for critical infrastructure operators (CIOs). It clarifies scope and governance expectations, and specifies compliance processes, marking a clear shift from principles to implementation. Although the CoP is not subsidiary legislation, it will be a central reference point for supervisory expectations and for any enforcement directions addressing non-compliance under the Ordinance.

What the CoP Is and How It Will Be Used

The CoP is not subsidiary legislation and non-compliance with it does not itself constitute an offence. However, the Commissioner may issue written directions with reference to the CoP's

The Global Regulatory Developments Journal / July–August 2026, Vol. 3, No. 4, pp. 311–316.

ISSN 2995-7486.

requirements, and failure to comply with such directions is an offence. In practice, the CoP functions as a compliance handbook against which CIOs can benchmark their cybersecurity governance and controls.

The CoP also indicates that designated authorities—currently the Hong Kong Monetary Authority and the Communications Authority—may adopt the CoP for category 1 and category 2 obligations and may issue sectoral codes in respect of those obligations where necessary.

What Is a Critical Computer System?

Under the Ordinance, a computer system that is accessible by the CIO in or from Hong Kong and is essential to the core function of a critical infrastructure operated by the CIO may be designated as a Critical Computer System (CCS). At first glance, this might appear to confer extra-territorial reach to the Ordinance. The Security Bureau has clarified this is not the case, although the Commissioner may request information accessible by a CIO in or from Hong Kong, whether located in or outside Hong Kong.

The CoP sets out indicators for CCS designation, including materiality to a critical infrastructure's core function, severe impact if disrupted, processing of sensitive digital data used directly in essential services, and strong dependencies with other CIOs (for example, centralised processing or data exchange systems across a sector or multiple sectors) or with other CCSs of the same CIO (for example, firewalls and backup facilities).

The CoP expressly brings industrial control systems within scope as computer systems, including supervisory control and data acquisition systems, distributed control systems and programmable logic controllers, recognising that operational technology can be mission-critical. It also indicates that underlying information technology infrastructure—such as network components, operating platforms, middleware, Internet-of-Things devices, and uninterruptible power supply systems—may be treated as components of a computer system.

To support a predictable designation process, the CoP lists the kinds of information regulators may request to determine a CCS designation, including (without limitation) the system's functions and dependencies (upstream and downstream), architecture and network diagrams, the nature and volume of sensitive digital data

processed, manufacturers and models, external service subscriptions, resilient setups, and design and operations descriptions.

Obligations for CIOs

The CoP provides practical guidance to help CIOs fulfil the three categories of obligations under the Ordinance: organisational (category 1), preventive (category 2), and incident reporting and response (category 3).

Category 1: Organisational Obligations

Under the Ordinance, a designated CIO must maintain an office in Hong Kong and must notify the relevant Regulating Authority in writing of any change of operator of a critical infrastructure within one month of the change.

The CoP clarifies that "maintain an office in Hong Kong" means carrying on actual business activities in Hong Kong (not merely having a correspondence address), such as managing daily operations and making business decisions. In relation to the obligation to set up and maintain a computer-system security management unit, the CoP clarifies that the unit and its supervising employee need not be based in Hong Kong. It also provides a non-exhaustive list of qualifications evidencing adequate professional knowledge in relation to computer-system security (for example, Certified Information Security Professional, Certified Information Systems Auditor) and links competence to professional experience commensurate with the risk profile of the CCSs. These are practical touchpoints not covered in the Ordinance.

Category 2: Preventive Obligations

The Ordinance requires CIOs to notify material changes to certain computer systems, and to submit and implement a computer-system security management plan, among other requirements. The CoP supplies operational detail and clarifies how CIOs should comply.

- *Material Changes Notification Triggers*. "Material changes" are changes reasonably expected to have a significant

effect on the security risk of a CCS or the risk to the core function of the relevant critical infrastructure. The CoP offers concrete examples of events that may constitute material changes, including platform migrations, major version upgrades of core components, changes to computing platforms or hardware, significant code changes, infrastructure alterations, and integration with or changes to interdependencies with external systems or networks.

- *Security Management Plan*. CIOs must submit and implement a computer-system security management plan covering all matters specified in Schedule 3 of the Ordinance, such as governance structure, policies and standards, risk management, access control, contracts and communications with suppliers, and personnel training. The CoP provides practical guidance on required content, sets out submission formalities, and requires a clear cross-reference mapping each applicable requirement to the relevant components of the plan and the corresponding sections of the CoP.
- *Security Audits*. A computer-system security audit is required to assess implementation of the security management plan and the security controls and measures adopted by the CIO. The CoP provides additional detail on auditor qualifications, recognised audit methodologies and standards, and the objectivity and impartiality of the audit process.

Category 3: Incident Reporting and Response

The CoP clarifies incident response obligations, including security drills, emergency response plans, and notification obligations.

- *Security Drills*. The Commissioner may, after giving reasonable written notice, require a CIO to participate in a security drill to test readiness to respond to computer-system security incidents. A CIO can be required to participate no more than once every two years. The CoP clarifies that drills will not require actual deployment of CCSs or involvement of production environments, to avoid disruption to business activities. It also outlines regulatory expectations, possible formats (for example, tabletop exercises, functional

exercises, simulated attacks), appropriate participants, and the post-drill feedback process.

- *Emergency Response Plan*. CIOs must submit an emergency response plan detailing protocols for responding to computer-system security incidents in respect of the CCSs of their critical infrastructures. The CoP clarifies that the plan must address incident management (for example, the emergency response team structure, statutory reporting requirements, triggering thresholds, communications plans, and procedural playbooks) and business continuity and disaster recovery (for example, business impact analysis, roles and responsibilities, employee training, recovery strategies and procedures). The plan should be endorsed at Board level or by a functional sub-committee delegated by the Board, or by senior management overseeing the operation of the relevant critical infrastructure. It should be reviewed upon material changes to CCSs and at least once every two years.
- *Incident Reporting Obligations*. The Ordinance sets incident notification timelines. The CoP further clarifies what constitutes a "computer-system security incident" by outlining relevant carve-outs and examples. Events arising from pure technical failure, natural disaster, mass power outage, a security threat that is detected and promptly removed or quarantined, or personal data leakage arising from human error do not constitute a computer-system security incident. Examples of incidents include large-scale or volumetric DDoS (distributed denial-of-service) attacks, ransom DDoS attacks, ransomware attacks that cause service suspension or show signs of data compromise, and malicious exfiltration of sensitive digital data. "Serious" incidents—which trigger the shorter reporting timeline of within 12 hours of awareness—are explained by reference to criteria such as service downtime exceeding (or likely to exceed) the maximum tolerable downtime defined in the business continuity management plan, minimum service levels being breached (or likely to be breached), leakage of a material volume of customer data, or receipt of attack threats from threat actors. Other computer-system security incidents not regarded as "serious" must be reported within 48 hours of the CIO becoming aware of the incident.

The CoP also clarifies the moment of awareness, tying it to a "reasonable degree of certainty" that an incident has occurred—a frequent operational question in breach response. Once that threshold is met, time starts to run for notification. Incidents must be notified within the prescribed timelines using the specified form and submitted via the designated secure channel. Alternatively, an initial notification may be made by telephone to the designated number, provided the specified form is submitted through the designated secure channel within 48 hours of that call. The CoP notes that other sector-specific incident notification requirements may apply in parallel.

Conclusion and Next Steps

The CoP clarifies governance expectations, technical baselines and operational processes under the new cybersecurity regime, and resolves key uncertainties—particularly around CCS designation, material change triggers, and incident-reporting thresholds and timelines. Although non-statutory in form, the CoP helps CIOs translate legal duties into implementable controls and measures, and anchors supervisory expectations that will be central to compliance audits and enforcement. The Commissioner may review and revise the CoP from time to time to reflect technological developments and industry best practice. Designated authorities may also issue sectoral codes for organisational (category 1) and preventive (category 2) obligations to reflect sectoral risk profiles and expectations.

Organisations that have been, or are likely to be, designated as CIOs should now treat the CoP as the operative compliance benchmark. They should implement structured programmes to align governance and controls with both the CoP and the Ordinance and closely monitor ongoing developments, including updates to the CoP, sectoral codes, and regulatory practices, to ensure timely adjustments to their compliance posture.

Note

* The authors, lawyers with Mayer Brown, may be contacted at gabriela.kennedy@mayerbrown.com and joanna.kc.wong@mayerbrown.com, respectively. Roslie Liu, legal practice assistant at Mayer Brown Hong Kong LLP, assisted with the preparation of this article.