Deloitte. 德勤

Protection of Critical Infrastructures (Computer Systems) Ordinance

What are the impacts on critical infrastructure operators?

November 2025

Leap Forward Bloom Beyond
勤躍香港 綻放未來

Protection of Critical Infrastructure (Computer Systems) Ordinance

With advancing information technology, **Critical Infrastructure (CI)** faces increasing **cyber threats. Protection of Critical Infrastructures (Computer Systems) Ordinance (the "CI Ordinance")** aims to enhance **Critical Computer System(CCS)** security, ensuring the **stable functioning** of **Hong Kong society** and **daily life**. Its **enactment** represents a **pivotal milestone** in **cybersecurity**, providing a reference for **future legislative efforts** while **reinforcing Hong Kong's legal framework**.

Two Categories of Critical Infrastructures

1 Necessary facilities for daily life

Energy	Information Technology	Banking and Financial Services	Air Transport
Land Transport	Maritime Transport	Healthcare Service	Telecoms and Broadcasting

2 Important Societal / economic facilities

Special Venues

Enterprises operating outside of the eight designated sectors may still be classified as CIs if their disruption could cause significant socioeconomic impact, subject to formal impact assessment.

Three Key Challenges and our Point of View

Upon the enactment of CI Ordinance, Critical Infrastructure Operators (CIOs) must address challenges and strive to achieve a balance between security compliance and efficient operations through strategic integration and technological innovation.

1 Is it mandatory to set up a security management unit in Hong Kong?

It is mandatory to establish and maintain a computer-system security management unit to oversee the security of critical computer systems and ensure compliance, while assuring the required expertise and culture are in place. However, the unit does not need to be physically located in Hong Kong, as long as it effectively covers the security oversight responsibilities for systems operating within Hong Kong.

2 Does the current management level meet the requirements of the CI Ordinance, and is the planning being conducted based on the CI Ordinance?

CIOs need to assess whether the existing management level can meet the requirements of the regulations, whether they can prevent and continuously detect incidents in advance, identify and respond promptly during incidents, and review and improve in a timely manner after incidents.

3 Is it necessary to consider a localization strategy?

Under the guidance of the Ordinance, CIOs need to gradually assess and evaluate its security architecture design, and take into considerations the resilient setup of the primary computer systems supporting core functions of the CI, such as localization strategy and implementation. CIOs also need to orchestrate the associated transition efforts to ensure effective adoption of the change in organization.

Road to Comply with CI Ordinance

Do Now

Compliance Gap Analysis

- Initiated immediately to allow sufficient time for rectification, ensuring that all compliance preparations are completed before the CI Ordinance officially comes into effect.

Do Next

Gaps Remediation

- Remediate the identified gaps based on the results of the gap analysis.
- For example, establishment of a security management unit and development of a security management plan.

2026

Designation of CIO

- Effective of the CI Ordinance
- Phase 1 CIOs will be assigned by first half of 2026

Do Later

Risk Assessment

within 12 months after the operator's designation date and conduct every 12 months

Computer System Security Audit

within 24 months after the operator's designation date and conduct every 24 months

Major Material Change submitted within 1 month after the occurrence of a major material change

Obligations of Critical Infrastructure Operator

A CIO will have three key categories of obligations:

Category 1 - Organisation

1 **Computer-System Security Management Unit**

Establish a dedicated computer system security management unit, **not required to be based in Hong Kong**, led by a qualified professional **with recognized certifications** (e.g., CISP, CISA, CISSP, CISM, or equivalent) to oversee the implementation, operation, and management of computer-system security for Critical Computer Systems (CCSs). The unit should possess the right capacity and capabilities to lead and reinforce compliance requirements, supported by augmented skills to drive organization-wide adoption.

Category 2 - Preventative

2 **Computer-System Security Management Plan**

Develop and review at least once every two years a robust security management plan incorporating a **risk management** structure that systematically identifies, assesses and monitors system risks. The plan establishes **clearly defined lines** of authority and roles, and aligns with the **control domains of the relevant Code of Practice (COP)**.

3 **Security Policy and Procedure**

Formulate enforce computer-system security policies, standards, and guidelines with **clear cross-reference mapping applicable requirements** that provide management direction and support for protecting CCS in alignment with business needs, security requirements, the COP, and relevant national and international standards.

4 **Security Measures for CCSs**

Implement security by design, asset management, access control, cryptography, system hardening, and patch management to **ensure system security throughout its lifecycle**.

5 **Security Measures for Operational technology (OT)**

Implement security by design, asset management, cryptography, password management and change management to **ensure OT system security throughout its lifecycle**. Alternative security measures are also provided when specified security requirements cannot be fulfilled.

6 **Risk Assessment, and Annual Reporting**

Perform **annual risk assessments**, including vulnerability scans and penetration testing, and conduct **independent security audits every two years**. Review protection levels, incidents, and improvement measures, and submit annual compliance reports.

7 **Security Training and Mindset**

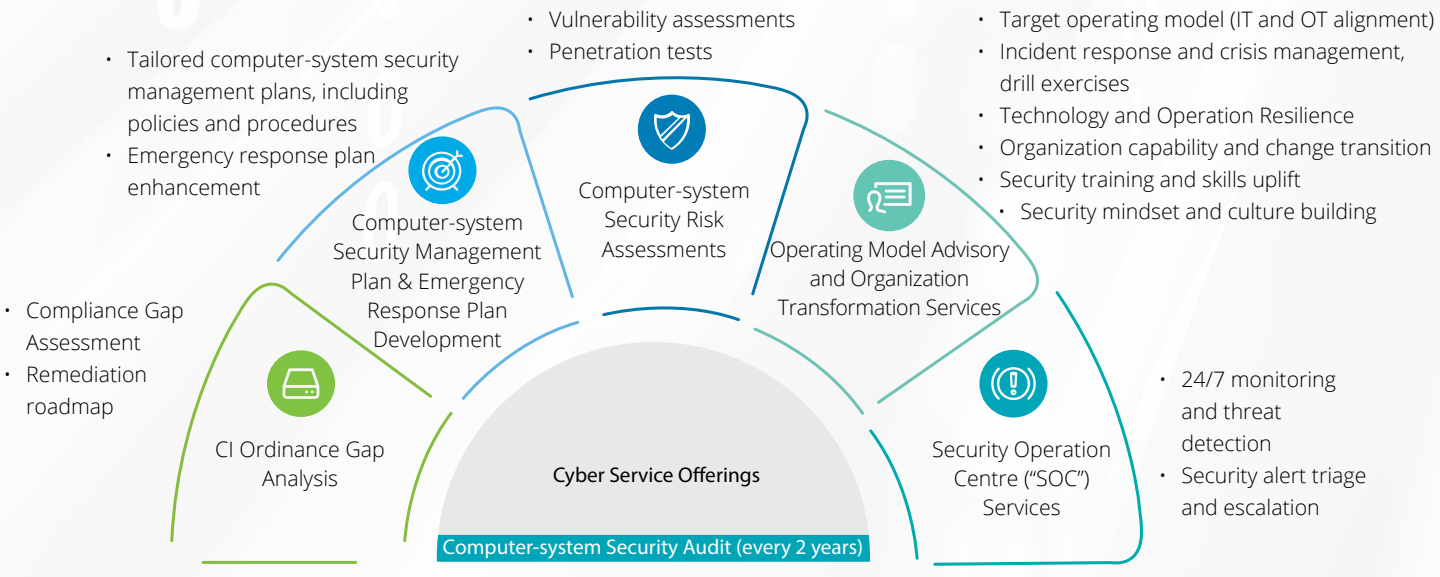
Provide **tailored training** for employees, suppliers, and contractors, covering cybersecurity awareness, incident response, and technical skills to ensure all personnel are **well-versed in compliance requirements**.

Category 3 - Incident reporting and response

8 **Incident Detection, Response, and Reporting**

Establish a monitoring mechanism to define normal behavior baselines and continuously detect anomalies. Participate in **computer system security drills every two years**, develop contingency plans, appoint 24/7 contact persons, report critical incidents within **12 hours** and other incidents within **48 hours**, and submit detailed written reports within 14 days. **Cooperate with the Commissioner** in responding to and investigating incidents, and comply with any written directions or requests issued by the Commissioner.

How Can Deloitte Help



What Unique Value Does Deloitte Provide

Enhanced Brand Reputation and Customer Trust
Proactive security measures build confidence with customers and stakeholders, protecting a company's image from the potentially devastating impact of a data breach.

Improved Operational Continuity and Resilience
Cybersecurity safeguards critical systems and data, ensuring that essential business operations can continue uninterrupted, even during and after a cyber incident.

Increased Revenue and Market Share
By ensuring the security of digital products and services, businesses can confidently pursue new revenue streams and expand into new markets, fostering growth.

Optimized Regulatory Compliance
Cybersecurity programs help organizations meet complex data protection regulations, avoiding penalties and building a strong compliance record.

Reduced Financial Losses
Effective security reduces the risk of costly breaches, fraud, and operational disruptions that can lead to significant financial damage.

Greater Operational Agility and Efficiency
Embedding security into the design of new services and technologies allows for faster, safer project rollouts and greater overall business flexibility.

Strategic Business Enabler
Cybersecurity evolves from a defensive function to a strategic partner, supporting innovation, digital transformation, and the secure adoption of new technologies.

Security-Conscious Workforce In Action
Strengthen organizational capabilities and change readiness for enhanced security practices, cultivating a security-first mindset and culture beyond technical proficiency.

Our Professionals' Qualifications

CISA CISSP CISM CRISC GCIH GCFA GCTI GDAT GREM CEH CHFI OSWE OSCE OSCP OSWP CREST

Our Success Stories

Our Deloitte Cyber professional team has the experience and knowledge to get you prepared for getting compliant with the CI Ordinance requirements. Below are some relevant successful stories of our technology & transformation practices on similar requirements across jurisdictions, which may also apply:

China Cybersecurity Law

- Assess the client's China operations, identify them as a Critical Information Infrastructure (CII) operator managing important data, and support MLPS certification for four systems under Level Protection 1.0 and 2.0 standards.
- Perform assessments against cybersecurity and data protection regulations in mainland China and Hong Kong, including CSL, PIPL, and PDPO. Recommend a tailored information security and data protection framework based on client circumstances.

Macau Cybersecurity Law

- Provide independent cybersecurity assessment services to identify gaps and recommend improvements, aligned with regulatory guidelines.
- Assess compliance with Macau Cybersecurity Law, MLPS standards, and AMCM circulars including Cyber Resilience and Critical Incidents Reporting, with support in regulatory submission/ notification processes.

Contacts

Allen Wong
Partner
Sales & Service
allewong@deloitte.com.hk

Sunny Ip
Partner
Engineering, AI&Data
sunip@deloitte.com.hk

Paul Sin
Partner
Fintech
paulsin-c@deloitte.com.hk

Steven Feng
Partner
Cyber Strategy & Transformation
stefeng@deloittecn.com.cn

Phill Everson
Partner
Technology & Transformation
philleverson@deloitte.com.hk

Andy Ng
Partner
Cyber Defense & Resilience
andycwng@deloitte.com.hk

Eileen Cheng
Partner
Cyber Strategy & Transformation
eicheng@deloitte.com.hk

Harry Wang
Partner
Cyber Defense & Resilience
harrywang@deloitte.com.hk

Sammie Shum
Partner
Organization & Change
sashum@deloitte.com.hk

Hatty Siu
Director
Cyber Strategy & Transformation
hattysiu@deloitte.com.hk

Phillip Mok
Director
Cyber Defense & Resilience
phmok@deloitte.com.hk

Chris Chui
Director
Cyber Defense & Resilience
cchui@deloitte.com.hk

Tony Lam
Director
Cyber Strategy & Transformation
tonlam@deloitte.com.hk