Implementing HK Critical Infrastructure Code of Practice Using ISO/IEC 27001

WHITE PAPER

SGS

SGS.COM

Introduction

In response to the escalating global threat of cyberattacks, the Security Bureau, Digital Policy Office (formerly the Office of the Government Chief Information Officer), and the Hong Kong Police Force jointly proposed a legal framework to regulate critical infrastructure operators (CI operators) and their Critical Computer Systems (CCS) in Hong Kong.

Following legislative review, the **Protection of Critical Infrastructure (Computer Systems) Bill** (the Bill) was passed by the Legislative Council on 19 March 2025 and will enact on 1 January 2026. The Bill establishes statutory requirements to enhance the protection of CCS across critical infrastructure (CI) sectors.

As outlined in Division 3 of Part 2 of the Bill, the regulatory authorities (the Commissioner and Designated Authorities) are empowered to issue a Code of Practice to provide CI operators with actionable guidance for complying with Category 1, 2, and 3 obligations[1].

On 14 July 2025, the Commissioner, in consultation with Designated Authorities, released a draft **Code of Practice Pursuant to the Protection of Critical Infrastructure (Computer System) Ordinance** for public consultation.

This article provides a comparison between draft Code of Practice and ISO/IEC 27001:2022 and explores how CI operators may consider adopting an internationally recognized ISO/IEC 27001 standard to serve as a management framework to implement the Bill so that a CI's CCS may be managed in a structured and systematically manner. The explanation and interpretation of the Bill and the Code of Practice is not the scope of this article. Readers of this article is advised to consult the Commissioner and the Designated Authorities for the requirements and their interpretations.

The comparison outlined in this article is based on the draft Code of Practice as of 14 Jul 2025. Updates may occur following the consultation period.

Structure of the code of practice

There are five core chapters in the Code of Practice in pursuant to the relevant sections in the Bill. Supplementary to these chapters, the annexes contain prescribed forms developed in accordance with the Bill's notification obligations.

Table 1:

THE CODE OF PRACTICE		THE BILL	
Chapter 3	Designation of critical computer systems	Section 13	Designating critical computer systems
Chapter 4	Information required for designation	Section 16	Requiring information for purposes of section 13
Chapter 5	Obligations of CI operator – Division 1	Part 4	Obligations of CI Operator – Division 1: Obligations relating to Organization of CI Operators
Chapter 5.1	Obligation to maintain office in Hong Kong	Section 19	Obligation to maintain office in Hong Kong
Chapter 5.2 Annex A	Obligation to notify operator changes Form for notifying changes of critical infrastructure operator	Section 20	Obligation to notify operator changes
Chapter 5.3 Annex B	Obligation to set up and maintain computer-system security management unit Form for notifying changes of appointment of employee supervising computer-system security management unit	Section 21	Obligation to set up and maintain computer-system security management unit
Chapter 6	Obligations of CI operator – Division 2	Part 4	Obligations of CI Operator – Division 2: Obligations relating to Prevention of Threats and Incidents

[1] Category 1 obligation: an obligation imposed by Division 1 of Part 4 (Obligations relating to Organization of CI Operators) of the Bill.
Category 2 obligation: an obligation imposed by Division 2 of Part 4 (Obligations relating to Prevention of Threats and Incidents) of the Bill and includes an obligation to comply with requirement imposed under section 24(5) or 25(4) or (6).
Category 3 obligation: an obligation imposed by Division 3 of Part 4 (Obligations relating to Incident Reporting and Response) of the Bill.

THE CODE OF PRACTICE		THE BILL	
6.1 Annex C	Obligation to notify material changes to certain computer systems Form for notifying material changes to certain computer systems	Section 22	Obligation to notify material changes to certain computer systems
6.2	Obligation to submit and implement computer-system security management plan	Section 23	Obligation to submit and implement computer-system security management plan
6.3	Obligation to conduct computer-system security risk assessments	Section 24	Obligation to conduct computer-system security risk assessments
6.4	Obligation to arrange to carry out computer-system security audits	Section 25	Obligation to arrange to carry out computer-system security audits
Chapter 7	Obligations of CI operator – Division 3	Part 4	Obligations of CI Operator – Division 3: Obligations relating to Incident Reporting and Response
7.1	Obligation to participate in computer-system security drill	Section 26	Obligation to participate in computer-system security drill
7.2	Obligation to submit and implement emergency response plan	Section 27	Obligation to submit and implement emergency response plan
7.3 Annex D	Obligation to notify computer-system security incidents Form for notifying computer-system security incident	Section 28	Obligation to notify computer-system security incidents

Alignment with ISO/IEC 27001 standard

Among all the requirements stated in the Code of Practice, Chapters 6.2 (Obligation to submit and implement computer-system security management plan) outlines the matters that shall be covered in the security management plan. When comparing the structure of this security management plan and requirements in Chapters 6.3 to 7.2, one may find that the plan and 6.3 – 7.2 shows many similarities and alignment to ISO/IEC 27001. The following table illustrates this correspondence:

Table 2:

THE CODE OF PRACTICE		ISO/IEC 27001	
Section	Guidance	Clause	Requirement
6.2.5 Computer-system security risk management approach	• The CI operator should formulate a systematic risk management approach to identify, assess, mitigate, and monitor the computer-system security risks of CCS	Clause 6.1.2 Information security risk assessment Clause 6.1.3 Information security risk treatment	An organization shall define and apply an information security risk assessment and treatment process to identify, assess, evaluate, and treat information security risks
6.2.6 Security by design	• The CI operator should adopt the security by design principle to ensure that security is an integral part of CCSs across its entire life cycle	A.8.25 Secure development life cycle A.8.26 Application security requirements A.8.27 Secure system architecture and engineering principles A.8.28 Secure coding	Rules for the secure development of software and systems shall be established and applied Information security requirements shall be identified, specified and approved when developing or acquiring applications Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities Secure coding principles shall be applied to software development

THE CODE OF PRACTICE		ISO/IEC 27001	
Section	Guidance	Clause	Requirement
		A.8.29 Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle
6.2.7 Asset management	• The CI operator should ensure an inventory of CCS and other associated assets is properly owned, kept, maintained, and restricted for access on a need-to-know basis	A.5.9 Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained
6.2.8 Access control and account management	• The CI operator should define and document procedures for approving, granting and managing user access to CCSs. The procedures should at least include user registration / de-registration, password delivery and password rest • Access rights should be reviewed at least once annually • Access rights should be revoked after a pre-defined period of inactivity or when no longer required • Unique user identity should be used. Shared or group user-IDs should not be permitted unless necessary	A.5.15 Access control A.5.16 Identity management A.5.17 Authentication information A.5.18 Access rights A.8.5 Secure authentication	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements The full life cycle of identities shall be managed Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control
6.2.9 Privileged access management	• The privileged access rights to CCSs are only provided with authorization	A.8.2 Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed
6.2.10 Cryptographic key management	• Cryptography should be used properly and effectively to protect the computer-system security of the CCSs • Cryptographic keys should be managed throughout their whole life cycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys	A.8.24 Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented
6.2.11 Password management	• The CI operator should define and implement password policies for all CCS accounts. The password policies should detail at least minimum password length, initial assignment, restricted words and format, and password life cycle	A.5.17 Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information

THE CODE OF PRACTICE		ISO/IEC 27001	
Section	Guidance	Clause	Requirement
6.2.12 Physical security	• The CI operator should prevent unauthorized physical access and interference to facilities housing CCS • Data centers and computer rooms should have physical security implemented to protect against computer-system security threats • Physical premises should be monitored by surveillance systems. • Access to building that house CCS should be continuously monitored to detect unauthorized access or suspicious behavior	A.7.1 Physical security perimeters A.7.2 Physical entry A.7.3 Securing offices, rooms and facilities A.7.4 Physical security monitoring A.7.5 Protecting against physical and environmental threats	Security perimeters shall be defined and used to protect areas that contain information and other associated assets Secure areas shall be protected by appropriate entry controls and access points Physical security for offices, rooms and facilities shall be designed and implemented Premises shall be continuously monitored for unauthorized physical access Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented
6.2.13 Configuration management and system hardening	• The CI operator should ensure the CCS align with the required security configurations • The baseline configuration of CCSs should be developed, maintained, and reviewed regularly	A.8.9 Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed
6.2.14 Change management	• Changes to CCSs should be subject to strict change management controls	A.8.32 Change management	Changes to information processing facilities and information systems shall be subject to change management procedures
6.2.15 Patch management	• The CI operator should protect their CCSs from known vulnerabilities by promptly applying the latest security patches	A.8.8 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken
6.2.16 Remote connection	• The CI operator should define appropriate usage policies and procedures specifying the security requirements when the CCSs are being accessed remotely from outside the CI operator's premises	A.6.7 Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises
6.2.17 Portable computing devices and removable storage media	• Strict security control should be in place over the connection of removable storage media and portable computing devices to CCSs	A.8.1 User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected
6.2.18 Backup and recovery	• The CI operator should formulate backup and recovery policies for their CCSs • Backup restoration tests should be conducted regularly	A.8.13 Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup

THE CODE OF PRACTICE		ISO/IEC 27001	
Section	Guidance	Clause	Requirement
6.2.19 Network security	• The CI operator should plan and implement adequate network security controls between the CCSs and the network • The CI operator should divide their networks into separated network domains based on trust levels	A.8.20 Network security A.8.22 Segregation of networks	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications Groups of information services, users and information systems shall be segregated in the organization's networks
6.2.20 Application security	• Unauthorized application software should not be loaded onto a CCS unless prior approval • The CI operator should establish and apply secure coding principles to the software development • The CI operator should conduct testing on the applications before it is released to production use • Test data should be carefully selected, protected and controlled	A.8.19 Installation of software on operational systems A.8.28 Secure coding A.8.29 Security testing in development and acceptance A.8.33 Test information	Procedures and measures shall be implemented to securely manage software installation on operational systems Secure coding principles shall be applied to software development Security testing processes shall be defined and implemented in the development life cycle Test information shall be appropriately selected, protected and managed
6.2.21 Log management	• The CI operator should record and identify the events of CCSs that can lead to a computer-system security incident concerning the CCSs • The CI operator should define policies relating to the logging of activities and log retention of CCSs	A.5.25 Assessment and decision on information security events A.8.15 Logging	The organization shall assess information security events and decide if they are to be categorized as information security incidents Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed
6.2.22 Cloud computing security	• The CI operator should define and document policies of CCSs for identifying, assessing, evaluating and responding to computer-system security risks associated with the adoption of cloud services	A.5.23 Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements
6.2.23 Supply chain management	• The CI operator should define and establish processes and procedures to manage the computer-system security risks with the products and services supply chain • The CI operator should maintain an agreed level of CCS security in supplier relationships • The CI operator should monitor and review with external service providers to ensure that operations having a potential effect on the computer-security risk of the CCSs by external service providers are documented and managed properly	A.5.19 Information security in supplier relationships A.5.20 Addressing information security within supplier agreements A.5.22 Monitoring, review and change management of supplier services	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery

THE CODE OF PRACTICE		ISO/IEC 27001	
Section	Guidance	Clause	Requirement
6.2.24 Monitoring and detection	• The CI operator should establish a mechanism to monitor the continuous operation of CCSs • The CI operator should establish mechanisms and processes to collect and analyze information relating to computer-system security threats to produce threat intelligence	A.8.16 Monitoring activities A.5.7 Threat intelligence	Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents Information relating to information security threats shall be collected and analyzed to produce threat intelligence
6.2.25 Computer-system security training	• The CI operator should formulate a training program to provide training periodically to all staff involved in CCS operation for their awareness and fulfilment of their computer-system security responsibilities • The CI operator should ensure the personnel of external service providers involved in CCS operation are provided with necessary computer-system security awareness training	A.6.3 Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function
6.3 Obligation to conduct computer-system security risk assessments	• The CI operator should refer to internationally recognized methodology and standards for computer-system security risk assessment such as ISO/IEC 27001, ISO/IEC 27005, NIST 800-30, etc. • The CI operator should maintain a computer-system security risk register and risk assessment report	Clause 6.1.2 Information security risk assessment Clause 6.1.3 Information security risk treatment	The organization shall define and apply an information security risk assessment and treatment process and shall retain the documented information
6.4 Obligation to arrange to carry out computer-system security audits	• The CI operator should arrange an independent auditor to conduct the computer-system security audit(s) for their CCSs	A.5.35 Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur
Annex F Outline methodology for the computer-system security audit	The audit is divided into the following stages: • Stage 1: planning • Stage 2: Fieldwork • Stage 3: Findings compilation • Stage 4: Reporting	ISO/IEC 27001 is a certifiable standard. A certification body, acting as an independent third party, conducts the certification audit in the following stages: **Stage 1: Document Review** The auditor evaluates the organization's Information Security Management System (ISMS) documentation to ensure alignment with ISO/IEC 27001 requirements. **Stage 2: Field Audit** The auditor assesses the implementation and effectiveness of the ISMS through interviews, evidence sampling, and process observations. At the closing meeting of the field audit, the auditor presents the audit findings to the audited organization. A formal audit report is then delivered within a specified timeframe	

THE CODE OF PRACTICE		ISO/IEC 27001	
Section	Guidance	Clause	Requirement
7.2 Obligation to submit and implement emergency response plan	• The CI operators should formulate emergency response plans to respond to computer-system security incidents • The plan should cover incident management and business continuity management and disaster recovery	A.5.24 Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities
		A.5.26 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures
		A.5.27 Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls
		A.5.28 Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events
		A.5.30 ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements

As a result of the comparison outlined above, a CI operator may find it beneficial to implement an information security management system (ISMS) according to ISO/IEC 27001 in order to effectively managing their CCSs such that meeting the Bill (and future Ordinance) is not a standalone exercise but is part of the CI operator's overall organization digital and cybersecurity framework.

CI operators already certified to ISO/IEC 27001

CI operators with existing ISO/IEC 27001 certification should conduct a comprehensive gap assessment to:

- Identify any requirements under the Code of Practice that have not been covered by their ISMS
- Prioritize remediation efforts to fill this gap
- Develop a roadmap for achieving full compliance with the Bill's provisions

This strategic approach ensures CI operators can build upon their ISO 27001 foundation while efficiently meeting the statutory requirements of the Bill.

Conclusion

As demonstrated by this article, the substantial alignment between the Code of Practice and the ISO/IEC 27001 requirements enhances the incentive and reduces the effort required for CI operators to implement the Code of Practice using ISO/IEC 27001 as a framework.

The standard facilitates the CI operator in developing, implementing, and maintaining a proven management framework to systematically and effectively complying to the Code of Practice. However, the readers are also reminded that Chapters 3 to 6.1 and Annex C have not been discussed and covered in this article. These Chapters are also needed to be implemented.

Disclaimer

The reader is reminded that SGS is not the authority or enforcement agency of the Bill and the future Ordinance. Implementation of an ISMS according to ISO/IEC 27001, or subsequent certification against this standard, does not imply that the CI has fulfilled all obligations of the Code of Practice. The information provided above is provided as a reference. This article should not be taken as an official interpretation of the Bill and the Code of Practice.

SGS Hong Kong Limited
Units 303 & 305, 3/F,
Building 22E, Phase 3,
Hong Kong Science Park,
New Territories,
Hong Kong

sgs.com

When you need to be sure