Compliance Brief

THALES

CYBERSECURITY

Complying with The Protection of Critical Infrastructures Bill in Hong Kong

cpl.thalesgroup.com

THALES

CYBERSECURITY

The Hong Kong Legislative Council passed the Protection of Critical Infrastructures (Computer Systems) Bill (the "CI Bill") on March 19, 2025, and it became effective on January 1, 2026. It is the first dedicated cybersecurity law in Hong Kong to protect the security of the critical computer systems (CCS) of critical infrastructures (CIs), to regulate CIs' operators (i.e., critical infrastructure operators (CIO)), and to provide for the investigation into, and response to, computer-system security threats and incidents.
The first version of the Code of Practice (CoP), released on January 1, 2026, by the Office of the Commissioner of Critical Infrastructure (Computer-system Security), provides practical guidance on how a CIO complies with category obligations..

What is the Protection of Critical Infrastructures (Computer Systems) Bill in Hong Kong?

Purpose

- To ensure the computer system security of critical infrastructure that is necessary for the normal functioning of the Hong Kong society
- To strengthen the security of the computer systems of critical infrastructure and minimize the chance of essential services being disrupted or compromised due to cyberattacks

Scope

- The regulation covers two major categories of critical infrastructure (CI):

Infrastructures for delivering essential services in Hong Kong covering eight sectors:

- Energy
- Information Technology
- Banking and Financial Services
- Land Transport
- Air Transport
- Maritime
- Healthcare Services
- Communications and Broadcasting

Other infrastructures for maintaining important societal and economic activities:

- Examples:
  - major sports
  - performance venues
  - research and development parks

- Critical Computer Systems (CCS)
  - CCSs refer to computer systems that are relevant to the provision of essential service of the core functions of computer systems, and those systems which, if interrupted or damaged, will seriously impact the normal functioning of the critical infrastructure.
- Critical Infrastructure Operators (CIO)
  - Designated operators which operate a Specified CI.

The Obligations of Operators Of Critical Infrastructure (CIO)

CIO will need to fulfill three types of obligations below:

Organizational

- maintain an address and office in Hong Kong
- report changes in the ownership and operatorship of CI
- set up a computer system security management unit with professional knowledge supervised by a dedicated supervisor of the CIO

Preventive

- inform the Commissioner's Office of material changes to their CCS
- formulate and implement a computer system security management plan
- conduct a computer system security risk assessment and audit (at least once every year and two years respectively)
- adopt measures to ensure that their 3rd-party services providers are in compliance with the relevant statutory obligations

Incident Reporting and Response

- participate in a computer system security drill (at least once every two years)
- formulate an emergency response plan
- notify the Commissioner's Office of the occurrence of computer system security incidents in respect of CCS

The Code of Practice (Code) of the **Protection of Critical Infrastructures (Computer Systems) Ordinance** is issued in respect of CIO obligations to set out recommended standards and provide practical guidance to CIOs to fulfil the obligations.

Regulatory authorities

The Chief Executive of Hong Kong appointed a new Commissioner of Critical Infrastructure (Computer-system Security), who, along with the designated authorities in Schedule 2 of the CI Bill for specific sectors (currently the Monetary Authority and the Communications Authority), ("Designated Authorities"), will serve as the regulating authorities.

Penalties

Concerning the relevant legislation of the UK and EU, the penalties under the Bill will only include fines, with a maximum level ranging from HK$500,000 to HK$5 million, and additional daily fines for persistent non-compliance for certain continuing offences, the maximum of which range from HK$50,000 to HK$100,000.

The obligations and requirements under the Bill which will result in offences and penalties for non-compliance will be imposed on CIOs at the organizational level only, and are not designed to target their staff at the individual level.

How Thales Helps with the Protection of Critical Infrastructures (Computer Systems) Ordinance Compliance

The Protection of Critical Infrastructures (Computer Systems) Ordinance (CI Ordinance) strengthens the cybersecurity of critical infrastructure and minimize disruption of essential services in Hong Kong; Thales' solutions can help CIOs address the requirements in the Code of the Ordinance by simplifying by simplifying compliance and automating security reducing the burden on security and compliance teams.

Address the requirements in CI Ordinance – The Code of Practice (The Code)

The Code	How Thales Helps	Solution Areas
6.2.8 – Security by Design (a) "… adopt the **"security by design"** principle… throughout their entire life cycle…"	• **Protect application data** and eliminate the need for Developers (Devs) to manage security and update data protection. • **Deploy data protection** solutions into environments through orchestration. • Perform updates and keep up with compliance requirements by **Data Security Admins** without taking Devs off of other projects. • Adopt **"Shift left"** – Security measurement in the early stage of development.	**Data Security** CipherTrust Data Security Platform Data Protection Gateway RESTful Data Protection Transparent Encryption for Kubernetes **Application Security** Elastic WAF (eWAF)
6.2.9 – Asset Management (b) "… ensure that up-to-date inventories … and the associated assets … are properly owned, kept, maintained, and restricted to access on a **need-to-know basis…**" (c) "… ensure the **accuracy of the inventories** of CCSs … by conducting **regular reviews** against the inventories or implementing automatic inventory update mechanisms…"	• **Discover and classify** potential risks for all public, private, and shadow APIs. • Identify **structured and unstructured sensitive data** at risk on-premises and in the cloud. • Enable **privileged user access control** for sensitive data and restrict access from unauthorized access with the least privileged design. • Identify the current state of **compliance, documenting gaps**, and providing a path to full compliance. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document.	**Application Security** API Security **Data Security** Data Activity Monitoring Data Discovery & Classification Data Risk Analytics Transparent Encryption

The Code	How Thales Helps	Solution Areas
6.2.10 – Access Control and Account Management (a) "… prevent unauthorised access and ensure that **only authorised personnel** can access CCSs…" (b) "… enforce **the least privilege principle** when assigning resources and privileges …" (c) "… define and document procedures…" (d) "…**User privileges and data access rights** should be clearly defined and reviewed…" (g) "…**Authorisation and authentication** measures commensurate … should be set up for each access. **Multi-factor authentication** should be adopted…"	• **Limit the access** of internal and external users to systems and data based on roles and context with policies. • Analyze access activity and deliver risk intelligence for IT teams to **proactively monitor** and investigate potential access risks. • Enforce data access rights and detect policy violations through **real-time monitoring**. • Apply **contextual security measures** based on risk scoring. • Prevent password fatigue with **Smart Single Sign-On** with conditional access. • Centralize **access policies** and enforcement to multiple hybrid environments in a single pane of glass. • Prevent **hardcoded credentials** or token keys in source code or CI/CD environments. • **Enable MFA** with the broadest range of hardware and software methods.	**Data Security** Data Activity Monitoring Data Risk Analytics Secrets Management Transparent Encryption **Identity & Access Management** Adaptive Access Multi-Factor Authentication Single Sign-On (SSO) Workforce Access Management
6.2.11 – Privileged Access Management (a) "… ensure the **privileged access rights** of CCSs are provided only with authorisation…" (c) "… enforcing the principle of **least privilege** for administrative accounts …" (d) "… allow only **authorised** devices equipped with security controls to access privileged accounts…"	• Provide **flexible authentication options** for automated workflows to mitigate the reliance on passwords. • Extend **single-sign-on authentication** to cloud applications, enabling centralized, secure access with a protected identity. • Apply **privileged access control** to sensitive data.	**Identity & Access Management** Workforce Access Management **Data Security** Transparent Encryption
6.2.12 – Cryptography (a) "… ensure proper and effective **use of cryptography** … "also refer to section 6.5.4 for the alternative security controls for an OT system…" (b) "…ensure the **cryptographic keys** are properly managed throughout their life cycle …" (c) "…Keys used to process sensitive digital data should be **stored and distributed separately**…" (d) "… refer to the **latest national and international**… cryptographic algorithms and methods …"	• Streamline **key management** on-premises and in the cloud environments with key lifecycle management. • Manage and **protect all secrets** and sensitive credentials. • Protect **cryptographic keys** in a FIPS 140-3 Level 3 environment. • Store encrypted data and its encryption **key stored in different places** for separation of duties principal. • Employ **strong** and **standard-based encryption protocols**, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. • Adopt **Post-Quantum Agility** to deal with the threats from quantum computing.	**Data Security** CipherTrust Data Security Platform Enterprise & Cloud Key Management Hardware Security Modules Post Quantum Cryptography Secrets Management

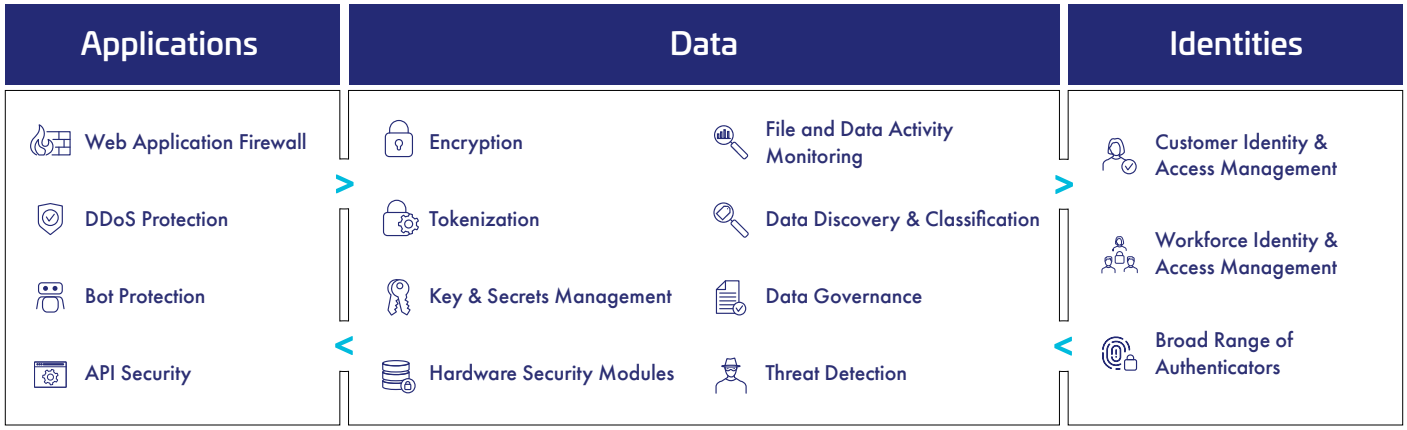
The Code	How Thales Helps	Solution Areas
6.2.14 – Physical Security (a) "… prevent **unauthorised physical access** and interference to facilities …" (b) "…Data centres and computer rooms housing CCSs should **implement physical** security…" (f) A list of personnel authorised to access data centres, computer rooms and other areas supporting CCS operations … should be **kept up-to-date and reviewed periodically.** All access keys, cards, passwords, etc., … should be physically secured and subject to well-defined and strictly enforced security procedures." **7.3.3 – Examples of computer-system security incidents…** (g) "… tampering with **cryptographic key management devices** that hampers the normal functioning …"	• Leverage **smart cards** for implementing physical access to sensitive facilities of critical infrastructure. • **Centralize access policies** and enforcement to multiple hybrid environments in a single pane of glass. • Protect the **root-of-trust** of a cryptographic system within a highly secure environment. • **Detect tamper events**, including unauthorized access to HSMs and key management infrastructure, through real-time audit logging and alerting.	**Identity & Access Management** Smart cards Workforce Access Management **Data Security** Hardware Security Modules
6.2.18 – Remote Connection (a) "… define appropriate usage policies and procedures … for **remotely accessing** the CCSs…" (b) "… implement suitable security measures to **prevent unauthorised** remote access to CCSs … implementing **multi-factor authentication…"**	• Enable **secure remote access** for resources on-premises or in the cloud with a seamless user experience. • Build and deploy adaptive authentication policies. • Enable MFA with the **broadest range** of hardware and software methods.	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication Workforce Access Management
6.2.21 – Network Security (a) "… plan and implement adequate network security controls … to prevent malicious traffic from accessing the CCS (e.g. **Denial-of-service ("DoS") attack**)." (b) "… install a network **intrusion detection** system or a network intrusion prevention system at critical nodes of the CCS…" **6.5.4 – Cryptography** (ii) "…protection for sensitive digital data in transit (e.g. encrypting data over networks) …" **6.5.7 – Network Security** (a) Alternative to section 6.2.21(a), … plan and implement adequate **network security controls** … to detect and manage **malicious traffic** from accessing the CCS.	• Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Detect and prevent **cyber threats** with web application firewall, ensuring seamless operations and peace of mind. • Secure **data-in-transi**t with future-proof encryption technologies to avoid "Harvest now, decrypt later".	**Application Security** Bot Protection Network DDoS Protection Cloud Web Application Firewall **Data Security** High Speed Encryption

The Code	How Thales Helps	Solution Areas
6.2.22 – Application Security (a) "… ensure the computer-system security … throughout the **development life cycle**…" (c) "…establish and apply **secure coding principles** … and remove any potential computer-system security **vulnerabilities** in the code…" (e) "…protect the **source code** from unauthorised access…" (f) "…Sensitive digital data should be removed or **masked** if it is used in the **testing environment**…"	• Protect apps from **runtime exploitation**, while integrating with tools in the CI/CD pipeline. • Stop **application attacks** with fewer false positives with web application firewall. • Safeguard critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • Conduct **ongoing risk assessments** to identify design flaws and vulnerabilities associated with the **OWASP** API Security Top 10. • **Encrypt sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized applications and personnel. • Protect and automate access to **secrets across DevOps tools**. • Easily access data security solutions through **online marketplaces**. • **Monitor data traffic** to spot data leakage risk.	**Application Security** API Protection Bot Protection DDoS Protection Runtime Protection Web Application Firewall **Data Security** Application Data Protection Database Encryption (TDE) DPOD Marketplace Secrets Management Tokenization
6.2.23 – Log Management (b) "… define policies for logging activities and **retaining logs** of CCSs to facilitate computer-system security incident investigations…"	• Provide **audit trails** of API calls, authentication attempts, and authorization decisions, ensuring accountability and facilitating compliance audits. • Produce audit trail and reports of all **access events** to all systems, stream logs to external SIEM systems. • **Prevent unauthorized access** and alteration to its internals, including the audit logs. • Gain visibility by monitoring and **auditing all database activity**. • Provide a **clear audit trail** for demonstrating cryptographic control from centralized key management systems, logging all key lifecycle events such as key creation, rotation, and access. • Offer **encryption logs**, data access attempts, and encryption/decryption events, providing auditable proof of data protection **without application modifications**.	**Application Security** API Protection **Data Security** Data Activity Monitoring Key Management Transparent Encryption **Identity & Access Management** Workforce Access Management

The Code	How Thales Helps	Solution Areas
6.2.24 – Cloud Computing Security (c) "… clearly define and implement the **shared responsibilities** for computer-system security of CCSs between the cloud service suppliers and the CI operator…" **6.2.25 – Supply Chain Management**	• Reduce **third-party risk** by maintaining on-premises control over encryption keys protecting data hosted in the cloud. • Ensure complete **separation of roles** between cloud provider admins and your organization, restrict access to sensitive data. • Monitor and **alert anomalies** to detect and prevent unwanted activities from disrupting supply chain activities. • Enable **relationship management** with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using **relationship-based fine-grained authorization**. • **Enable MFA** for third-party users to thwart phishing attacks. • Apply **sufficient secure measurement** with the sensitivity of data. • **Protect network tunnel** between cloud and on-premises environment to ensure data is encrypted.	**Identity & Access Management** Delegated User Management Externalized Authorization Risk and Threat Evaluation Third-party Access Control Workforce Access Management **Data Security** Cloud Key Management Data Activity Monitoring Data Discovery and Classification High Speed Encryption Transparent Encryption User Rights Management
6.2.26 – Monitoring and Detection (a) "… establish a mechanism to monitor the continuous operation … for **detecting anomalies** and potential computer-system security incident…" (e) "… establish mechanisms and processes to collect and analyse information related to computer-system security threats … produce threat intelligence."	• Monitor I/O and block **suspicious activity** before ransomware can take hold. • **Prevent malicious** software and users from accessing sensitive data. • Use signature, behavioral and reputational analysis to **block all malware** injection attacks. • Detect and prevent cyber threats with **web application firewall**. • Safeguard critical network assets from **DDoS attacks and Bad Bots**.	**Application Security** Bot Protection DDoS Protection Web Application Firewall **Data Security** Data Risk Intelligence Ransomware Protection
7.3.3 – Examples of computer-system security incidents (d) "… employee accesses to **sensitive digital data** of a CCS and maliciously exfiltrates that data or maliciously misconfigures the access privilege of the CCS…"	• **Detect data exfiltration** in real-time through behavioral analytics and anomaly detection to identify abnormal data access patterns. • **Monitor data activity** to track unauthorized downloads, copies, or transfers of sensitive customer information. • **Encrypt sensitive data** at rest and in transit to minimize the impact of data leakage, ensuring leaked information remains unusable. • **Classify and discover** sensitive customer data across the environment to ensure proper protection and visibility. • Generate **audit trails** for all data access events to support forensic investigation and regulatory incident reporting.	**Data Security** Data Activity Monitoring Data Discovery and Classification File Activity Monitoring Transparent Encryption

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

Security for What Matters Most



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, APIs, and a secure Content Delivery Network (CDN).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Disclaimer: The information contained herein is believed to be accurate on the date of publishing. Thales provides this material for your information only. Its content is not legal advice nor does it amount to a certification or guarantee of compliance in respect of any applicable law. Third parties shall be solely responsible for their own interpretation of any applicable law. The information should not be construed as a commitment to deliver any specific upgrade, feature or functionality. You should not rely on the anticipated timelines or potential upgrades, features or functionality described in the presentation when making a decision to purchase products from Thales. Thales does not accept any liability howsoever arising from any use of this material.

© Thales - January 2026 • EHv17