WHITE PAPER

# How to Prepare for Hong Kong's Protection of Critical Infrastructures Bill in 2026

## Ensuring Compliance and Strengthening Supply Chain Resilience

SecurityScorecard

# Table of Contents

# Executive Summary

Hong Kong's critical infrastructure sectors face an increasingly complex cyber risk landscape. Global threat activity, rising regulatory expectations, and the need to safeguard essential public and economic functions have accelerated the development of a far more robust cybersecurity framework in the region. The Protection of Critical Infrastructures Bill, which took effect on January 1, 2026, reflects this shift, positioning supply chain protection as a critical component of national resilience whilst introducing a structured, accountability-driven approach to securing critical computer systems.

While CIOs and CISOs retain overall responsibility, they aren't the only ones under scrutiny; under the new legislation, compliance extends to risk, cybersecurity, and assurance teams. Now, these functions must work collectively to identify vulnerabilities, assess operational exposure, and implement measures that reduce the likelihood, and impact, of nationwide disruption.

As stated in the Hong Kong Security Bureau's explanatory notes, responsible parties must *"address risks arising from reliance on external service providers and ensure resilience of outsourced or interconnected systems."*

Automation, continuous monitoring, and structured governance processes will be essential for meeting the requirements of The Protection of Critical Infrastructures Bill and embedding long-term resilience across critical operations. To best prepare, organizations should look to achieve real-time visibility across internal systems and third-party environments, a clear understanding of their digital footprint, and the capability to assess and act on emerging risks.

## Supply Chain Resilience Is on the Global Agenda

The Bill aligns Hong Kong's approach with international regimes; jurisdictions worldwide—including Australia's Security of Critical Infrastructure (SOCI) Act, the EU NIS2 Directive, Singapore's Cybersecurity Act, the Digital Operational Resilience Act (DORA), and the U.S.'s Executive Order 14028 on Improving the Nation's Cybersecurity—are increasingly introducing legislation that emphasize operator-level accountability for external dependencies and brings supply-chain security firmly within regulatory scope.

# Who is in Scope?

The Bill applies to designated operators of critical infrastructure and to the computer systems required to deliver their essential services. It covers organizations operating in key sectors, including:

- Energy
- Information Technology
- Banking & Financial Services
- Communications & Broadcasting
- Land, Air, and Maritime Transport
- Government and Public Services
- Healthcare Services

The scope includes any critical computer system, regardless of whether it is internally managed, outsourced, or interconnected with external partners. This extends to cloud platforms, managed service providers, and third-party technologies.

The inclusion of external systems reflects the nature of modern operations, where digital ecosystems are intricately tied and supply-chain dependencies extend well beyond an organization's traditional perimeter.

With up to 82% of global security leaders having significant concern about the security of their supply chain, more than 70% of organizations experiencing third-party cyber incidents, and more than a third of all data breaches being tied to third-party systems, it's unsurprising that there is demand for these sectors to maintain better visibility and tighter control across their broader digital and supply-chain ecosystem.

## The Cost of Non-Compliance

Beyond a drastically increased cyber risk, non-compliance carries significant financial penalties, ranging from HK$500,000 to HK$5 million, with additional daily fines for ongoing breaches.

These obligations apply at the organizational level, not the individual, reinforcing the need for formal governance structures, documented risk assessments, and proactive oversight of third-party environments.

# What the Legislation Means for Organizations

The Bill significantly broadens cybersecurity obligations, signaling a clear shift in how organizations are expected to manage their cyber risk.

Crucially, critical infrastructure operators must now implement comprehensive risk management, including formal risk assessments, cybersecurity management plans, and documentation of mitigation actions and controls. These requirements apply to all systems fundamental to service continuity, whether internally operated or managed by external providers.

Explicit obligations for third-party and supply-chain oversight have also been introduced. Vendors, contractors, managed service providers, and cloud partners fall within this regulatory perimeter, and operators remain accountable for risks flowing from these relationships.

Effective compliance requires involvement from risk, compliance, and assurance teams, and is no longer the sole responsibility of CIO and CISO oversight. Expectations include due diligence, continuous monitoring, contractual controls, and demonstrable supplier oversight.

As of January 2026, regulators will have broad authority to request third-party audits, system reviews, and contractual amendments. As with international frameworks such as NIS2, DORA, and Singapore's Cybersecurity Act, the Bill requires a shift from ad-hoc practices to evidenced, continuous governance supported by structured processes and documentation.

## Financial Services and Banking

Financial institutions operate in highly interconnected environments where core functions depend on a complex mix of cloud platforms, fintech providers, managed services, and outsourced infrastructure. These dependencies increase exposure to third-party cyber risk, making it far more difficult to maintain consistent security standards across the ecosystem. Under the Bill, financial institutions must demonstrate not only that controls are in place, but that they are effective, continuously monitored, and responsive to emerging threats.

Given the sector's systemic importance, regulators are likely to place particular emphasis on operational resilience, vendor oversight, and evidence of ongoing risk management. This includes understanding concentrations of risk across critical suppliers, monitoring externally exposed assets, and ensuring that disruptions in third-party environments do not cascade into customer-facing or market-wide impacts.

## Healthcare Services

Healthcare providers rely on a diverse mix of clinical systems, administrative platforms, and connected medical devices, many of which were not designed to address modern cyber threats. Legacy infrastructure, combined with the growing digitization of patient services, creates unique vulnerabilities that can affect both data protection and patient safety.

The Bill heightens the importance of availability, integrity, and continuity of care, requiring operators to maintain visibility across clinical technologies, external service providers, and specialized vendors. Compliance will depend on demonstrating that cyber hygiene is consistently maintained across all systems that support patient outcomes, and that risks are identified and mitigated before they disrupt care delivery.

## Energy and Utilities

Energy and utility providers support essential services where cyber incidents can have immediate and widespread societal consequences. These organizations often operate in converged OT/IT environments, supported by industrial control systems, specialized vendors, and geographically distributed infrastructure. The Bill reinforces the need to manage cyber risk across these complex operational landscapes.

Compliance will require continuous oversight of systems that support generation, transmission, and distribution, along with clear governance of third-party access and dependencies. Operators must be able to demonstrate control over interconnected environments and show that vendor-related risks are actively managed to prevent service outages or cascading failures.

## Transport (Air, Land, Maritime)

Transport operators depend on tightly integrated systems for scheduling, navigation, communications, and logistics. These systems often rely on third-party technologies and service providers, creating layered dependencies across national and international supply chains. Cyber incidents in this sector can disrupt passenger services, freight movement, and critical trade routes.

The Bill places greater emphasis on maintaining operational continuity across complex, multi-stakeholder environments. Transport operators will now need to demonstrate structured risk management across operational technologies and external partners, ensuring that vulnerabilities in interconnected systems do not compromise safety, reliability, or service availability.

## Information Technology, Communications, and Broadcasting

These sectors provide the digital backbone that supports other critical infrastructure operators. High levels of interconnectivity, shared platforms, and data center dependencies mean cyber incidents can have cascading effects beyond the originating organization.

Following the introduction of the Bill, organizations in these sectors must maintain strong visibility across their external attack surface and third-party relationships, alongside robust vulnerability management practices. Compliance will depend on the ability to identify emerging risks quickly, manage dependencies across interconnected networks, and demonstrate ongoing oversight of systems critical to national connectivity and the flow of information.

## Government and Public Sector

Government entities operate systems that deliver essential public services and manage sensitive citizen data, often across a mix of internally managed platforms and outsourced services. These systems are highly visible and subject to heightened public and regulatory scrutiny, particularly where service disruptions could at best affect public trust or at worst impact public safety.

There is now a call for clear governance, documented risk management, and continuous oversight across both internal and external systems. Public sector organizations must be able to demonstrate how risks are identified, managed, and mitigated across their digital ecosystem, ensuring continuity of services and accountability at the organizational level.

# Compliance Challenges Organizations Must Overcome

The Protection of Critical Infrastructures Bill introduces governance expectations that require organizations to demonstrate a far more consistent, evidence-driven approach to cybersecurity than they have historically had to.

While many operators already maintain baseline controls, meeting the requirements of the Bill demands greater visibility, continuous oversight, and clearer accountability across both internal environments and extended supply-chain ecosystems. The breadth of the Bill means that gaps which were previously manageable—such as limited visibility over external assets or inconsistent supplier oversight—now represent material compliance risks.

To align with the new regulatory expectations, organizations must overcome several structural and operational challenges. The following sections outline the most significant challenges and the areas where organizations will need to strengthen capability to ensure resilience and compliance under this new legislation.

## Visibility into Externally Exposed Risks

Organizations frequently lack full visibility over exposed assets, including shadow IT, misconfigurations, and unknown systems. Without continuous oversight, vulnerabilities across dispersed digital environments may go unaddressed. These include:

### Identifying Blind Spots

Managing risk across extensive third- and fourth-party environments is a persistent challenge. Distributed supplier ecosystems make it difficult to evaluate security posture, track remediation progress, and identify hidden dependencies.

### Demonstrating Compliance

The Bill requires operators to produce clear evidence of governance, mitigation, and oversight. Board -level accountability means organizations must maintain structured reporting for regulatory inquiries and internal assurance.

### Maintaining Control

Annual or periodic assessments are insufficient due to evolving threats and the dynamic nature of digital ecosystems. Organizations need real-time insights and automated mechanisms to ensure controls remain effective over time.

# How SecurityScorecard Supports Compliance with The Protection of Critical Infrastructures Bill

Meeting the requirements of The Protection of Critical Infrastructures Bill demands continuous visibility, clear governance evidence, and effective oversight of increasingly complex supply-chain environments.

The scale of these obligations—combined with operator-level accountability for both internal and outsourced systems—means organizations require capabilities that go beyond periodic assessments or manual controls. Tools that integrate external telemetry, third-party risk intelligence, and automated workflows are becoming essential to meeting regulatory expectations.

SecurityScorecard provides these capabilities in a single platform. Continuous monitoring, real-time insight into external attack surfaces, and structured third-party oversight enable organizations to identify vulnerabilities early, prioritize remediation, and maintain an auditable record of governance activities. The platform supports the shift from reactive, point-in-time processes to continuous, data-driven assurance, directly aligning with the principles embedded in the Bill.

By combining internal security insights with supply-chain risk intelligence, SecurityScorecard helps operators manage exposure across their entire digital ecosystem and act before risks materialize. This enhances both compliance readiness and operational resilience, ensuring organizations are better positioned to address evolving threats and regulatory scrutiny.

## Continuous Cyber Hygiene Monitoring for Internal and External Assets

SecurityScorecard provides continuous oversight of external digital assets, identifying vulnerabilities, misconfigurations, and emerging threats. Capabilities such as supply chain visibility and proactive risk visualization support prioritization and early mitigation in line with regulatory expectations.


## External Telemetry Across the Digital Footprint

External telemetry provides automatic digital assets discovery, mapping the attack surface without manual input to identify exposures across internet-facing systems, cloud infrastructure, and public applications. This outside-in visibility supports early detection and proactive remediation, supported by tools such as the cyber risk heatmap.

## Third-Party and Supply-Chain Risk Management

SecurityScorecard continuously monitors third-party and supply-chain partners, issuing alerts when vendor security posture declines. Organizations can proactively identify the effects of supply chain incidents across their entire vendor ecosystem and use remediation workflows to engage suppliers and address risks collaboratively.

## AI-Driven Supply Chain Cyber Risk Management

SecurityScorecard provides AI-enabled analytics detect vulnerabilities across third- and fourth-party ecosystems, uncover hidden dependencies with extra low false positives (less than 1%), and automate workflows to enhance supply-chain oversight. The integration of HyperComply provides further automation for security reviews and compliance processes, supporting vendor assurance.

## Evidence for Regulatory Assurance

SecurityScorecard produces structured, auditable reporting that aligns with the Bill's documentation requirements. Reports demonstrate risk assessments, mitigation timelines, and continuous oversight, supporting both regulatory submissions and internal governance. Certifications and supporting regulatory evidence from vendors can align with external threat intelligence to provide a complete view of risk.

## Benchmarking and Board Oversight

The platform provides benchmarking against sector baselines and clear, measurable risk insights for executive and board audiences. This facilitates informed decision-making and demonstrates ongoing governance maturity and oversight. Improved hygiene of an organization's supply chain can be viewed through traceable insights using benchmarking and board level data.

# Recommendations and Next Steps

Preparing for The Protection of Critical Infrastructures Bill requires organizations to adopt a structured, forward-looking approach to governance, risk management, and supply-chain oversight.

The priority now is to establish clear baselines, strengthen visibility across both internal and external systems, and embed processes that support continuous, auditable compliance. The following steps outline practical, immediate actions that operators can take to build readiness ahead of enforcement and to establish a sustainable compliance posture.

SecurityScorecard is uniquely positioned to accelerate, streamline, and simplify these steps, helping organizations guarantee readiness and properly demonstrate compliance.

**1. Conduct a Pre-Compliance Readiness Assessment**
Identify critical systems, suppliers, and areas of concentrated risk to establish a baseline for compliance and mitigation.

**2. Implement Continuous External Monitoring**
Move beyond periodic assessments to continuous, real-time visibility into vulnerabilities and third-party exposures.

**3. Strengthen Supplier Governance Models**
Update contractual requirements, onboarding processes, and oversight mechanisms to ensure third-party alignment with cybersecurity expectations.

**4. Build a Sustainable Reporting Framework**
Develop dashboards, metrics, and reporting processes aligned with regulatory requirements to support ongoing internal and external assurance.

# Preparing for Resilience in 2026 and Beyond

Hong Kong's Protection of Critical Infrastructures Bill represents a significant shift toward proactive, organization-wide accountability, reflecting similar legislation that is rapidly being introduced globally.

Organizations that act now can transform regulatory obligations into an opportunity to strengthen operational resilience, safeguard essential services, and demonstrate accountability to regulators and stakeholders alike. Delaying preparation increases exposure to operational disruption, regulatory fines, and reputational risk.

SecurityScorecard equips organizations with the intelligence, automation, and oversight needed to meet these challenges. From continuous monitoring of internal and external assets to AI-driven supply chain risk management to actionable reporting for boards and regulators, SecurityScorecard helps organizations identify vulnerabilities, enforce standards across third-party ecosystems, and maintain real-time assurance of compliance.

By adopting these capabilities ahead of January 2026, affected organizations can confidently navigate the new regulatory landscape while building a more resilient, secure future.

To ensure you comply with The Protection of Critical Infrastructures Bill and create your free account, visit SecurityScorecard.com

SecurityScorecard is transforming how organizations defend against the fastest-growing threat vector – supply chain attacks. Our industry-leading security ratings serve as the foundation and core strength, while our AI-powered (or threat-informed) TPRM solutions continuously monitor third-party risks using our factor-based ratings, automated assessments and proprietary threat intelligence, to resolve threats before they become breaches. MAX enables response and remediation capability, working through our service partners to protect the entire supply chain ecosystem while strengthening operational resilience, enhancing third-party risk management, and mitigating concentrated risk.

Trusted by over 3,000 organizations—including two-thirds of the Fortune 100—and recognized as a trusted resource by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io