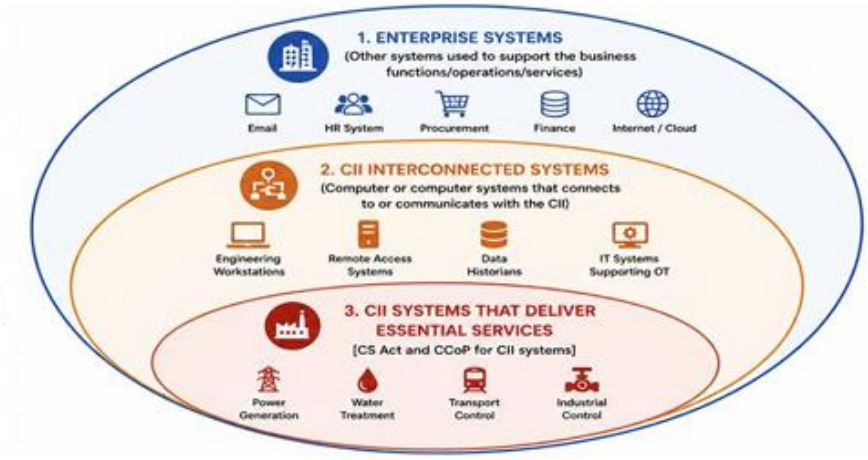
STEPHENSON HARWOOD
(Singapore) Alliance

September 2026

SINGAPORE'S CSA ISSUES UPDATED CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE

On 29 July 2026, Singapore's Cyber Security Agency ("**CSA**") issued the updated Cybersecurity Code of Practice for Critical Information Infrastructure (the "**Code**"). The updated Code represents a significant enhancement in Singapore's approach towards Critical Information Infrastructure ("**CII**") protection, such as imposing board-level accountability on CII owners ("**CIIO**") and mandating Cyber Trust Mark certification (Tier 5) for all CIIO and their auditors.

The updated Code also extends the scope of application for specific cybersecurity obligations to interconnected information technology or operational technology systems or network infrastructure owned, operated, and/or controlled by the CIIO, but which are not themselves designated as CII ("**Interconnected Systems**"). In addition, the Code annexes various recommendations for components of an IT or OT system and/or network infrastructure owned and controlled by the CIIO that support the CIIO's business, operational or administrative functions and services ("**Enterprise Systems**"), which fall outside the scope of mandatory CII requirements, to strengthen the overall cybersecurity posture.



Source: Cyber Security Agency of Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure 2026

The Code takes effect on 29 July 2026 (the "**Effective Date**"). Most new obligations take effect on 29 July 2027 (the "**Compliance Date**"), while existing CIIOs are required to attain Cyber Trust Mark Advocate (Tier 5) certification (or its equivalent) by 31 December 2027. The Code is issued by the Commissioner of Cybersecurity (the "**Commissioner**") pursuant to section 35A(1)(a)(i) of the Cybersecurity Act 2018 (the "**Act**"). Under section 35A(6), CIIOs are required to comply with the Code. With effect from the Effective Date, the Code supersedes the previous version of the Code. The requirements under the Code are to be read together with, and are in addition to, the CIIO's other obligations under the Act and any other applicable laws, as well as any relevant written directions or other codes of practice issued by the Commissioner under the Act.

This article highlights the key changes introduced by the Code from the previous Cybersecurity Code of Practice for Critical Information Infrastructure (Second Edition), issued on 4 July 2022 (as revised on 12 December 2022) (the "**2022 Code**"), and their implications for CIIOs.

KEY DATES

Effective Date: 29 July 2026

Compliance Date (most new obligations): 29 July 2027

Cyber Trust Mark certification deadline (existing CIIOs): 31 December 2027

GOVERNANCE REQUIREMENTS

Board-level accountability

The Board's Terms of Reference or mandate must include overseeing the organisation's cybersecurity risk posture and providing strategic direction and guidance to Senior Management on the management of cyber risks.

The Board's accountability and direction must be evidenced through a documented cyber resilience framework covering four pillars: (i) Risk Tolerance, requiring the issuance and maintenance of a cyber risk appetite statement; (ii) Risk Mitigation, requiring oversight of the cybersecurity budget and resource allocation; (iii) Risk Transfer, requiring oversight of cyber risk transfer arrangements, including cyber insurance; and (iv) Risk Recovery, requiring oversight of the Business Continuity and Disaster Recovery strategy defining the organisation's maximum tolerable downtime following a cyber incident or disruption to the provision of essential services. All four pillars must be reviewed at least annually (or more frequently, based on the evolving cyber threat landscape), with each review and any resulting update to the Board documented in Board minutes or equivalent written records.

Board members must now participate in annual contextualised cybersecurity training that covers, at a minimum, the strategic oversight and governance of cybersecurity risks, and regulatory compliance obligations under the Act and other applicable legislation and codes of practice. Such training must be delivered by an internal or external subject matter expert and conducted at least once every 12 months, or as often as required based on the evolving cyber threat landscape. Newly appointed Board members must complete this training within 12 months of their appointment and should be supported through regular cybersecurity briefings in the interim. Board members are also required to receive cyber threat briefings every six months (or as often as needed based on the evolving cybersecurity threat landscape), from senior management.

Each briefing must address, at a minimum: (i) cyber threats relevant to the CII, the CIIO organisation and the CIIO's sector; (ii) any threats actively targeting the CII, the CIIO organisation and/or the sector since the last briefing; and (iii) the implications of those threats for the CIIO's cyber risk posture, including any recommended changes to controls, risk appetite, cybersecurity budget or resource allocation.

Senior management responsibility

At least one member of senior management, or an individual working in or for the CIIO (for example, a designated Chief Information Security Officer) must possess the knowledge and awareness necessary to manage cyber risks across the CII, its interconnected systems and the CIIO's enterprise network, provide oversight of cybersecurity

measures, and ensure their appropriate implementation.

The senior management roles and organisational structure must be set out in writing, specifying responsibilities and authority for incident reporting and escalation, incident investigation, cyber risk trade-off decisions, and cybersecurity policy and resource approval.

In addition to the separate cyber threat briefings described above, senior management must provide the Board with regular reports on the organisation's cybersecurity posture, risks and reportable incidents affecting the CII, interconnected systems and the CIIO's enterprise network at least every 6 months, and promptly upon any reportable incident or material change to the CIIO's cyber risk profile. All reports and related deliberations must be documented in Board minutes or equivalent written records.

Senior management is required to allocate adequate resources and budget for cybersecurity, commensurate with the cyber risks facing the CII, its interconnected systems and the CIIO's enterprise network. The adequacy of such resources and budget must be reviewed at least once every 12 months, or following any material change to the CIIO's cyber risk profile, and the outcomes of the review must be documented.

Cyber trust mark certification (Tier 5)

Cyber Trust Mark Advocate (Tier 5) is the highest cybersecurity preparedness tier under CSA's Cyber Trust Mark programme, which serves as a risk-based framework for organisations to implement cybersecurity practices and measures commensurate with their cybersecurity risk profile. The scope of certification must encompass the CIIO's governance, risk management, and enterprise-wide management of cybersecurity capabilities, system operational processes, and information systems and infrastructure that the organisation owns, operates, and/or controls, which are used to deliver its products and services.

A CIIO must be certified with Cyber Trust Mark Advocate (Tier 5) or its equivalent within 24 months of its designation as an owner of CII systems. Existing CIIOs must be certified by 31 December 2027. The CIIO must ensure that its certification remains valid and that the audit firm it engages to perform the cybersecurity audit under Section 15 of the Act is certified with Cyber Trust Mark Advocate (Tier 5) or its equivalent.

RESPONSE AND RECOVERY REQUIREMENTS

Cybersecurity exercise

CIIOs must establish a cybersecurity exercise plan comprising: (i) a Master Scenario Events List, which is a chronological sequence of simulated events and injects designed to guide exercise play, prompt participant actions, and test whether the exercise objectives are achieved; and (ii) the full exercise schedule, including communication protocols, rules of engagement, and post-exercise review processes to capture lessons learned and inform ongoing improvements. If requested by the Commissioner, the CIIO must submit a copy of the exercise plan for review to the Commissioner within 30 days of receiving the request.

Scenario-based cybersecurity exercises should be developed based on threat modelling methodologies such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege), and test the effectiveness of the following plans. The exercise scenarios should include both CII systems and interconnected systems, based on the exercise objectives and scope, to ensure holistic evaluation of cybersecurity readiness:

- Crisis Management Plan for decision-making (Led by the CEO or a member of the Senior Management team);
- Cybersecurity Incident Response Plan (led by the CISO or a suitably qualified personnel);
- Sectoral Heightened Alert Plan (led by the CISO or a suitably qualified personnel);
- Business Continuity Plan (led by the CIO or a suitably qualified personnel);
- Disaster Recovery Plan (led by the CIO or a suitably qualified personnel);
- Internal and External Stakeholders Communication Plan (led by the Head of Communications or a suitably qualified personnel); and

+ Improvement Plan(s) from previous exercise reviews (led by the CISO or a suitably qualified personnel).

CIIOs are required to conduct scenario-based cybersecurity exercises with the relevant stakeholders (e.g. the crisis management team, CIRT, business operation staff, crisis communication and external parties) at least once every 12 months and the first instance of such exercises must be completed no later than 12 months after the Compliance Date. If requested by the Commissioner, the CIIO must submit a copy of the completed cybersecurity exercise report, together with its post-exercise improvement plans, to the Commissioner within 30 days of receiving the request.

CIIOs must also assign personnel responsible for the cybersecurity of the CII to participate in technical cybersecurity exercises organised by CSA or its designated partners at least once every 12 months.

EXTENSION OF MANDATORY CYBERSECURITY CONTROLS TO INTERCONNECTED SYSTEMS

Previously, the 2022 Code's mandatory requirements applied only to systems designated as CII. In practice, however, threat actors have increasingly exploited less-monitored systems adjacent to the CII. The extension of certain mandatory cybersecurity controls to Interconnected Systems is intended to close such gaps.

The updated Code introduces seven categories of mandatory requirements for Interconnected Systems to protect them from being exploited as attack vectors into the CII environment:

1. **Asset management.** CIIOs must identify all interconnected system assets and maintain an inventory covering, for each asset, the owner and/or operator, name and description, critical functions, key persons responsible for cybersecurity, dependencies and connections with any internal or external systems or networks, physical location, outsourced service providers, cloud services used, and internet links supporting the asset (including any distributed denial-of-service (DDoS) attack mitigation measures in place). CIIOs must also maintain an accurate CII network topology diagram identifying the interconnected systems and the interfaces and connectivity between the network devices and segments.

2. **Account management.** Each account must be granted only the minimum privileges necessary for its assigned functions, any account that is no longer necessary or is inactive must be deleted or disabled to prevent unauthorised access, and all accounts (including privileged, user and application accounts) must be reviewed at least once every 12 months.

3. **Privileged account management.** Multi-factor authentication is now required for privileged accounts on Interconnected Systems, sharing of privileged accounts is prohibited, and break-glass account usage must be logged and reviewed.

4. **Network segmentation.** Interconnected Systems must be segmented into different network segments based on their security and risk levels. Firewalls must be implemented at the boundaries between interconnected systems, and between internet-facing assets and the enterprise environment, permitting only authorised traffic through defined firewall rules. Unauthorised outbound network connections from interconnected systems must be monitored and blocked.

5. **System hardening.** Only ports, services and protocols necessary for the operations of the interconnected systems may be enabled, and unused ports, services or protocols on internet-facing devices (such as routers, firewalls and VPN gateways) must be disabled.

6. **Patch management.** Security patches must be applied in a timely manner, with compensating controls where patching is not immediately feasible.

7. **Monitoring and detection.** CIIOs must monitor network management activities, endpoint detection logs, and virtualised environments (including vCenter and ESXi hosts) across interconnected systems. CIIOs must also ensure that the virtualisation management infrastructure—including

vCenter Servers and ESXi hosts—runs supported versions and is fully patched, with compensating controls where updates or patches cannot be applied. Suspicious activities must be reported to CSA under the National Cybersecurity Incident Reporting Framework — a new obligation that previously applied only to incidents affecting the CII itself. All monitoring mechanisms must be reviewed at least annually.

OTHER AMENDMENTS - "IF REQUESTED BY THE COMMISSIONER"

Another noteworthy amendment is that several of the existing requirements that have remained largely unchanged – Threat Hunting, Incident Management, and Crisis Communication Plan - have been updated to provide that the CIIO shall, if requested by the Commissioner, submit a copy of the relevant report to the Commissioner no later than 30 days upon receiving the request.

For Monitoring and Detection, the CIIO shall also facilitate, if requested by the Commissioner, the deployment of CSA-supported threat detection systems across designated segments of the CIIO's network.

CONCLUSION

The updated Code marks a significant increase in regulatory expectations for CIIOs by strengthening CII governance, visibility, detection and readiness, and extending mandatory controls to Interconnected Systems. CIIOs should use the transition period between the Effective Date (29 July 2026) and the Compliance Date (29 July 2027, or 31 December 2027 for Cyber Trust Mark certification) to:

+ conduct a gap analysis of their existing cybersecurity governance framework against the new Board-level accountability and senior management responsibility requirements;
+ identify and document all Interconnected Systems and begin implementing the seven mandatory control categories;
+ develop or update their cybersecurity exercise plans, including the Master Scenario Events List;
+ engage with CSA-accredited certification bodies to plan for Cyber Trust Mark Advocate (Tier 5) certification; and
+ review and update internal policies and procedures to address the Commissioner's expanded powers to request reports and facilitate threat detection deployments.

The updated Code is expected to be followed by the release of a Cybersecurity Code of Practice (Cloud) governing the secure deployment, operation and management of CII systems hosted on the cloud; however, the Code does not specify when the Cloud CCoP will be released.

CONTACT US

SHEETAL SANDHU

Partner at Virtus Law

+65 6661 6523
sheetal.sandhu
@stephensonharwood.com

SHU WEI LEE

Associate at Virtus Law

+65 6661 6893
shuwei.lee
@stephensonharwood.com

With thanks to Avryl Chaar, Corporate Trainee Solicitor, for her assistance on this article.

The Singapore law aspects of this article were written by members of Virtus Law (a member of the Stephenson Harwood (Singapore) Alliance).