ENSIGN
INFOSECURITY

Ensign’s Cybersecurity Guide on the Second Edition of the Cybersecurity Code of Practice (CCoP 2.0) for Critical Information Infrastructure (CII)

SEPTEMBER 2022

Background

CII systems in Singapore provide essential services for the sustenance and growth of the country, such as water, energy, healthcare, and transport, amongst others. A cyber-attack targeted on the CII can have detrimental and/or systemic impact on the country's economy and society. Hence, the CCoP for CII was first introduced in 2018 to provide a framework for CII Owners (CIIOs) with the objective to strengthen their cybersecurity posture and enhancing their cyber resilience.

However, the threat landscape continues to evolve. Threat actors are adopting new and more sophisticated tactics and techniques in their malicious cyber operations. These include the use of Wiperware, Misinformation, Disinformation, Malinformation (MDM), and cyber supply chain compromise, making it more difficult for CIIOs to safeguard their CII systems.

Considering this, the Cyber Security Agency of Singapore (CSA) has published the CCoP 2.0 for CII which came into effect on 4 July 2022, superseding the previous versions of the code. Its aim is to establish stronger governance and strengthen cyber resiliency in the 11 CII sectors.

For existing CIIs, compliance date would be 12 months from the date of designation of this code. However, with respect to a newly designated CII, compliance date would be 12 months from the date of designation.

Shift from Compliance to Risk-based Approach in the New CCoP

CCoP 1.0
(Sep 2018)

Compliance-based approach

Setting basic cyber hygiene practices

Addendum 1
(Dec 2019)

OT-specific security requirements

Mandatory requirements to elevate OT cybersecurity

CCoP 2.0
(Jul 2022)

Risk-based approach

Focuses more on threat and risk-based approach

Structured into 7 policy domains which further split into 5 domains applicable to all CIIOs, 1 specific to OT CIIOs and 1 for other domain

Addresses cyber risk of emerging technologies such as cloud computing

Details OT security requirements

Incorporates practices from industry standards such as NIST CSF, MITRE Cyber Resiliency Techniques, SingHealth COI and PSDSRC

Key Changes and Ensign's Recommendations

We have summarised the key changes in the revised CCoP in the table below. Through Ensign's suite of cybersecurity services and capabilities, we can help CIIOs mitigate cyber threats, manage cyber risks, and become compliant with the new code.

KEY CHANGES IN CCoP 2.0	WHAT YOU NEED TO DO	HOW ENSIGN CAN HELP
1 Involvement of Board of Directors and Senior Management in cybersecurity matters References: 3.1.2, 3.1.3	■ Board of Directors must include at least one personnel who provides guidance to senior management on systemic cybersecurity risks. ■ Senior management team includes an individual who understands cybersecurity risks.	■ Board Simulation Exercises on Cybersecurity Risk Management, and Cyber Incident and Crisis Management ■ Cybersecurity capability and capacity profiling ■ Target Operating Model design addressing People and Organisation design, processes and cybersecurity technology architecture
2 Specific risk assessment methodology References: 3.2.1, 3.2.2, 3.2.3	■ For OT systems, perform hazard analysis and apply remediation controls. ■ Include non-digital engineering controls as mitigation in OT systems, where applicable.	■ Risk management framework review ■ Risk assessment services for IT and/or OT system(s) ■ Develop risk methodology and controls for continuous monitoring ■ Advisory service to reduce risk & business impact ■ Threat modelling and Risk profiling
3 Detailed focus on design principles References: 3.5.1, 3.5.2	■ Apply defence-in-depth security architecture to prevent any point of failure. ■ Adopt zero-trust principles before granting access.	■ Secure system architecture review ■ Security-by-design and processes development

KEY CHANGES IN CCOP 2.0	WHAT YOU NEED TO DO	HOW ENSIGN CAN HELP
4 Cloud Security References: 3.7.1, 3.7.2, 3.7.3	■ Must notify the Commissioner about the implementation of CII on the Cloud, irrespective of deployment model (public, private or hybrid) or service model (SaaS, IaaS and PaaS). ■ Conduct cybersecurity risk assessment for cloud services if CIIO has plans to implement CII, wholly or partially, on the Cloud. ■ Must submit the cybersecurity risk assessment report to the Commissioner within 30 days of its completion. ■ Ensure that Cloud service provider appoints a person within Singapore for service and legal process, if any.	■ Cloud security risk assessment service ■ Advisory service to evaluate threat, risk, and impact for risk management ■ Deploy Cloud Identity Access Management to identify over-privileged identities for IaaS environment approved for CII. ■ Deploy Cloud Security Posture Management to ensure security best practices are deployed and monitored for Cloud environment approved for CII.
5 Strengthen Vendor Management References: 3.8.2, 3.8.3	■ Establish processes to maintain oversight over all outsourced functions or services. ■ Include clause in the agreement to reduce or mitigate the impact of any cybersecurity risks associated with outsourced services. ■ Include clause in the agreement which gives CIIO the right to audit vendors' cybersecurity postures in relation to outsourced services. ■ Establish vendor compliance framework.	■ Vendor cybersecurity risk assessments and audit ■ Compliance review

KEY CHANGES IN CCOP 2.0	WHAT YOU NEED TO DO	HOW ENSIGN CAN HELP
6 Enhanced Asset Management Reference: 4.1.1	■ Incorporate additional criteria to asset inventory such as: a. Dedicated cybersecurity person for each CII asset b. Description of internet links including DDoS mitigation measures	■ Asset management policy review and processes development ■ Asset discovery and management
7 Heightened Privileged Access Control Reference: 5.3.1	■ Establish privileged access management practice. ■ Implement MFA for privileged users.	■ Identity and access management policy review and processes development ■ Implement and operate privileged access management with multi-factor authentication to enforce strong password management and remote access to the CII environment.
8 Monitor Domain Controllers Reference: 5.4.1	■ Establish process to monitor domain controllers for possible compromise.	■ Implement domain controller security monitoring to identify anomalies in real time.
9 Database security References: 5.13.1, 5.13.4, 5.13.5	■ Establish database security processes including securing data at rest, and preventing data exfiltration. ■ Monitor database and bulk queries to identify anomalies if they breach the predetermined threshold.	■ Database policy review and processes development ■ Understand database monitoring needs, and deploy and manage necessary database access management solutions.

KEY CHANGES IN CCOP 2.0		WHAT YOU NEED TO DO	HOW ENSIGN CAN HELP
10	Adversarial attack simulation exercise References: 5.16.1, 5.16.2	■ Establish Red Teaming and/or Purple Teaming attack simulation plans. ■ Regularly conduct whole-of-business cyber scenario-based exercises.	■ Cyber Simulation Exercises (Cyber Range, Tabletop and Wargame) ■ Red/Purple Teaming with intelligence on sectoral context ■ Security Testing (VA/PT). ■ Implement breach attack simulation for continuous Red Teaming. ■ Compromise assessments
11	Cryptographic Key Management Reference: 5.17	■ Implement cryptographic key lifecycle management and M-of-N key access.	■ Design and implement Public Key Infrastructure (PKI) lifecycle with Certificate Practice Statement. ■ Implement Key Management System and Hardware Security Modules to protect cryptographic keys.

KEY CHANGES IN CCOP 2.0	WHAT YOU NEED TO DO	HOW ENSIGN CAN HELP
12 Comprehensive focus on logging, detection, threat hunting and threat intelligence References: 6.1, 6.2, 6.3, 6.4	■ Collect various types of logs such as network firewall logs, DNS logs, web proxy logs and NIDS/NIPS logs. ■ Actively participate in threat intelligence sharing. ■ Perform behavioural analysis.	■ Log management and incident management policy review and processes development ■ Cyber Threat Intelligence monitoring services ■ Threat Intelligence Platform ■ IT/OT SOC Design, build and operate ■ Managed Security Services (including Managed Detection and Response Services) ■ Ad-hoc Threat Hunting service ■ User and Entity Behaviour Analytics (UEBA) ■ AI-Powered Cyber Analytics Anti-Phishing and Anti-Ransomware solutions ■ Information sharing and threat analysis policy and processes development ■ Threat models development
13 Detailed guidance on backup and restoration Reference: 8.1	■ Establish backup and restoration process. ■ Perform periodic backup and restoration testing.	■ Backup and restoration policy review and processes development

KEY CHANGES IN CCOP 2.0	WHAT YOU NEED TO DO	HOW ENSIGN CAN HELP
14 Cybersecurity skills Reference 9.2.3	■ Require Certified in Risk and Information Systems Control (CRISC) or equivalent certificate to supervise cybersecurity risk assessment for CII. ■ Require Certified Information Systems Auditor (CISA) or equivalent certificate to supervise cybersecurity audit for CII.	■ Certified risk assessor/ auditor to perform cybersecurity risk assessment and cybersecurity audit for CII ■ Cybersecurity Competency Training
15 Specific focus on OT Security References: 10.2, 10.3, 10.4	■ OT CII should not be connected with the enterprise network unless approved, and direction of data flow is restricted to only one-way (OT CII to the enterprise network). ■ Develop fail-safe mechanism to minimise disruption to operations. ■ Establish field controller security.	■ Cybersecurity architecture review ■ Security-by-design and Zero Trust Architecture principles application to OT architecture ■ Cybersecurity management processes development for OT incident response and recovery ■ Static and dynamic application security testing ■ OT visibility and security monitoring tool deployment and integration into OT SOC
16 Domain Name System (DNS) Security Reference: 11.2	■ Implement DNSSEC, or equivalent or better methods to validate the integrity of DNS records.	■ Advisory service to DNSSEC enablement ■ Deploy DNSSEC and PKI to internal DNS architecture.

About Ensign

Ensign InfoSecurity is the largest pure-play, end-to-end cybersecurity service provider in Asia. Headquartered in Singapore, Ensign offers bespoke solutions and services to address their clients' cybersecurity needs. Our core competencies are in the provision of cybersecurity advisory and assurance services, architecture design and systems integration services, and managed security services for advanced threat detection, threat hunting, and incident response. Underpinning these competencies is in-house research and development in cybersecurity. Ensign has two decades of proven track record as a trusted and relevant service provider, serving clients from the public and private sectors in the Asia Pacific region.

For more information, you may visit www.ensigninfosecurity.com or contact us at marketing@ensigninfosecurity.com

ENSIGN
INFOSECURITY