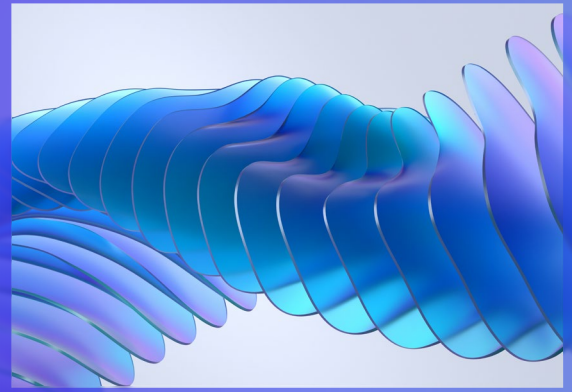


Track your Critical Information Infrastructure Obligations with the CII Monitoring Tool (CMT)

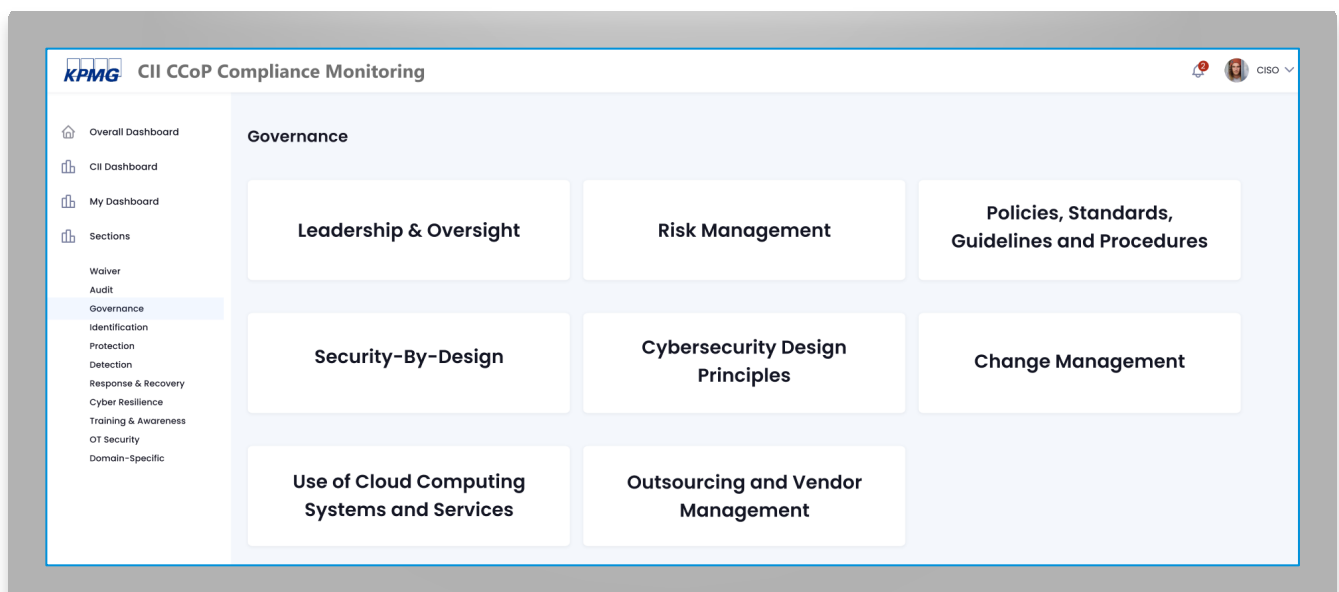


As Critical Information Infrastructure (CII) owners embark on their cybersecurity journey, adhering to a multitude of regulatory requirements can prove to be a tall order. With the frequency, volume and severity of cyber attacks increasing, organisations will need to ensure that their systems are cybersecure to stay resilient.

Due to the need to monitor compliance of multiple assets against the Cybersecurity Code of Practice (CCoP), KPMG's CII Monitoring Tool (CMT) provides a centralised platform solution to help organisations track governance, risk and compliance for CII assets.

CII owners can benefit from deploying such a centralised platform solution because it is typically difficult to track the various obligations under the CCoP such as assessment timelines, remediation actions, responsible parties and etc., especially when a client has numerous CIIs under their purview. With CMT, timeline tracking and reminders can be automated, along with providing a dashboard status overview for management.

Illustrative Samples



Illustrative Samples (Cont'd)

KPMG CII CCoP Compliance Monitoring
User1

- Overall Dashboard
- CII Dashboard
- My Dashboard
- Sections
- Audit
- Governance**
- Leadership and Oversight
- Risk Management
- Policies, Standards, Guidelines and Procedures
- Security-by-Design
- Cybersecurity Design Principles
- Change Management
- Use of Cloud Computing Systems and Services
- Outsourcing and Vendor Management
- Identification
- Protection
- Detection
- Response & Recovery
- Cyber Resilience
- Training & Awareness
- OT Security
- Domain-Specific

Governance – Leadership and Oversight

Governance involves establishing and maintaining frameworks to ensure that the CIO's cybersecurity strategies are aligned with its business objectives. It also provides guidance to the CIO in evaluating, defining, and directing efforts to manage cybersecurity risks. Adequate resources and attention must be devoted to the CIO's cybersecurity strategy and its application to the CII. Effective leadership from the board of directors and senior management is essential in building the right organisational culture, mindset, and structure towards cybersecurity, and to provide effective and timely business decisions on important cybersecurity matters.

S/N	CONTROL STATEMENT	TO DO	FREQUENCY	TYPE	CII	DUE DATE	LAST UPDATED DATE	TAGGED TO	STATUS
3.1.1(a)	The CIO shall ensure that the roles relevant to ensuring the CII's cybersecurity are set out in writing, and the responsibility for each of these roles is assigned to a person working in or for the CIO. This document shall: (a) Specify the organisational structure for persons involved in managing and ensuring the cybersecurity of the CII;	Maintain a document that specifies the organisational structure for persons involved in managing and ensuring the cybersecurity of the CII.	Quarterly	Manual Update	CII 1	2023-03-31	2022-12-21	User 1	Non-Compliant
3.1.1(b)	The CIO shall ensure that the roles relevant to ensuring the CII's cybersecurity are set out in writing, and the responsibility for each of these roles is assigned to a person working in or for the CIO. This document shall: (b) Ensure that the organisational structure prevents conflicts of interest from arising in relation to decisions relevant to the cybersecurity of the CII;	Maintain a document that sets clear segregation of duties.	Annual	Manual Update	CII 1	2023-12-31	2022-12-11	User 1	Compliant

KPMG CII CCoP Compliance Monitoring
CISO

- Overall Dashboard
- CII Dashboard
- My Dashboard
- Sections
- Audit
- Governance**
- Leadership and Oversight
- Risk Management**
- Policies, Standards, Guidelines and Procedures
- Security-by-Design
- Cybersecurity Design Principles
- Change Management
- Use of Cloud Computing Systems and Services
- Outsourcing and Vendor Management
- Identification
- Protection
- Detection
- Response & Recovery
- Cyber Resilience
- Training & Awareness
- OT Security
- Domain-Specific

Governance – Risk Management

The purpose of conducting this annual cyber risk assessment is to enable the Company to:

- Identify "what could go wrong" cyber events that are often a result of malicious acts by threat actors and could lead to undesired business consequences;
- Determine the levels of cybersecurity risk that they are exposed to. A good understanding of the risk levels would allow an organisation to dedicate adequate actions and resources to treat risks of the highest priority; and
- Create a risk-aware culture within the Company. Risk assessment is an iterative process that involves engaging employees to think about technology risks and how they align to business objectives.

Risk Assessment Status

	LAST PERFORMED ON	STATUS	DUE DATE	PENDING ACTION FROM
CII 1	2023-04-30	In progress	Due in 1 month	User 1
CII 2	2022-12-01	Initiating	> 3 months	User 2
CII 3	2022-12-01	In progress	Due in 3 months	User 3

Open Risk Treatment

- In Progress **10**
- Urgent Pending **3**
- To Assign **2**

Risk Treatment Items

S/N	SYSTEM	ACTION ITEM	PENDING ACTION FROM	DUE DATE
RM-00001	CII 1	Adversary exploits a vulnerability on the API or Webservices (e.g. through fuzzing on API) enabling the adversary to gain access to the Compensation application system. Adversary modifies the input data resulting in inaccurate compensation information leading to loss of trust and reputation damage.	User 1	2023-07-21
RM-00004	CII 3	Adversary gains unauthorised privileged access to the database by using a default password to exfiltrate confidential information.	User 3	2023-07-21
RM-00004	CII 3	Adversary exploits vulnerabilities in system, due to weak programming or logic flaws to exfiltrate confidential CII data accessed and used by these applications.	User 3	2023-07-21

Join us as a pilot participant for our CMT programme.

- Pilot participants will co-fund the development of a Beta version and might receive incentives for it. The pilot can be conducted together with participants based on their requirements and preferences with regards to what information is useful for them. This includes options like interface design and workflow processes.
- A typical timeline for a pilot trial is 3 months.
- Subsequent clients who come onboard after the pilot trial will be charged on a subscription basis.

Contact us

KPMG Services Pte Ltd

12 Marine View, #15-01
Asia Square Tower 2
Singapore 018916
T: +65 6213 3388
F: +65 6225 0984

Eddie Toh

Partner
Cyber,
Advisory
KPMG in Singapore
T: +65 6213 3028
E: eddietoh@kpmg.com.sg

Kan Shik Kiong

Director
Cyber,
Risk Consulting
KPMG in Singapore
T: +65 6213 3699
E: shikkiongkan@kpmg.com.sg

Joe Chan

Director
Cyber,
Risk Consulting
KPMG in Singapore
T: +65 6213 3051
E: joechan3@kpmg.com.sg

Matt Loong

Associate Director
Cyber,
Risk Consulting
KPMG in Singapore
T: +65 6213 3274
E: mattloong@kpmg.com.sg

kpmg.com.sg



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.