ANNEX 2: Comparison in Approaches Towards CII Organizations – Singapore, China, and Thailand

Jurisdiction	Criteria for CII Organization	Summary of Obligations	Additional Notes
Singapore	An entity is designated as an owner of CII if it is designated by the Commissioner of Cybersecurity, based on the following criteria: (a) the computer or computer system is necessary for continuous delivery of an essential service (found in First Schedule of Singapore's Cybersecurity Act and cutting across a variety of industries e.g., energy, info-communications, healthcare, transport, etc.); (b) the loss or compromise of computer or computer system will have debilitating effect on availability of essential service in Singapore; and (c) the computer or computer system is located wholly or in part in Singapore.	Key obligations include: • Establishing mechanisms and processes to detect cybersecurity threats and incidents. • Reporting cybersecurity incidents to Commissioner of Cybersecurity. • Conducting regular cybersecurity audits and risk assessments of CII. • Furnishing necessary information on e.g., design, configuration and security of CII to the Commissioner of Cybersecurity upon written request.	• Singapore also has the Personal Data Protection Act which requires organizations to put in place reasonable security measures to protect personal data under its possession and/or control. • Recent amendments to Singapore's Personal Data Protection Act (including additional subsidiary legislation through the Personal Data Protection (Notification of Data Breaches) Regulations 2021) create reporting obligations if a data breach meets certain thresholds.
China	CII Organizations are defined as follows: (a) organizations operating in certain prioritized industries (including finance, medicine and health, public communications, information services, energy, transportation, etc.), important internet application systems; and "operators of other critical Information Infrastructure";	Key obligations include: • Establishing a comprehensive network security protection system and accountability system; • Setting up a dedicated security management function and designate a person-in-charge; • Carrying out network security	• The focus when deciding on CII Organization status appears to rest on the impact of a data security breach, e.g., where a data incident involving an organization may affect, e.g., a substantial percentage of the population of a city, or if an organization handles and

Jurisdiction	Criteria for CII Organization	Summary of Obligations	Additional Notes
	(b) by reference to a risk of harm test, namely where a security breach of the infrastructure operated by the organization may cause significant consequences/ potential impact. CII Organizations will be designated by their respective industry regulators, and will be notified if they are deemed to be CII Organizations.	inspections and risk audits at least once a year; • Implementing emergency plans for cybersecurity events and carry out routine emergency drills; and • Reporting network security incidents to regulators.	processes very sensitive personal information, e.g., relating to government officials that may have national security implications. • Other factors should also be considered in assessing whether an entity is a CII Organization e.g., types and amount of data collected, stored, or processed by an organization, the data processing activities it undertakes, the organization's operations and infrastructure etc.
Thailand	Organizations private or public with characteristics as prescribed by the National Cybersecurity Committee (the "**NCC**"), which has operations or missions relating to: • National security; • Substantive public service; • Banking and finance; • IT and telecommunications; • Transportation and logistics; • Energy and public utilities; • Public health; or • Other characteristics as prescribed by the NCC.	Key obligations include: • Observing compliance with the CSA Code of Practice and standard framework for maintenance of cybersecurity. • Examining its operations to ensure the organization complies with the minimum cybersecurity standard prescribed by the Supervising Organization. • Conducting annual risk assessments on "maintaining cybersecurity." These assessments	• Thailand also has its Personal Data Protection Act, which requires an organization's "Data Controller" to put in place appropriate security measures to protect and store personal data. • An organization has a reporting obligation to the relevant authorities if a "cyber threat" results in a data leak.

Jurisdiction	Criteria for CII Organization	Summary of Obligations	Additional Notes
		should be conducted by information security auditors, internal auditors or external independent authorities, and the results should be submitted to the Office of the NCC. • Reporting to the Office of the NCC and relevant Supervising Organization upon being subject to a "cyber threat."	