

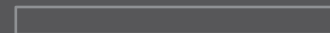
# Risk-Based Protection of Critical Information Infrastructure

A Policymaker's Guide



# Contents

- 2 1. Introduction
- 5 2. Critical Information and Infrastructure Regulations
- 15 3. Principles for Approaching Critical Information Infrastructure Regulations Proportionately
- 30 4. Summary: Recommendations for Approaching Critical Information Infrastructure Management
- 32 5. Critical Information Infrastructure Considerations Checklist



# 1. Introduction

Digital transformation and the importance of digitalization have been key to many governments' modernization efforts. In the wake of the COVID-19 pandemic, there has been an acceleration of efforts to ensure that critical infrastructure (CI) and the information services which serve them are able to continue running in the event of another global catastrophe and remain resilient against potential disruptions.

In the process of developing the necessary policies and regulations to protect these essential services, many governments—particularly developing countries—have started their digitalization journeys, where many ministries and departments have used information and communication technologies (ICTs) to create efficiencies and increased efficacies in their citizen services and governmental operations.

Examples where digital technology services are present in essential services:

## Infrastructure



Where industrial control systems (ICS) are used to electronically control and manage tasks efficiently in utilities

## Shared Services



Where digital identities and service records are managed and stored in a central database

## Financial Services



Where payment switches facilitate transactions between users, merchants, acquirers, and banks

The focus on protecting public service infrastructure has therefore become increasingly important, and a class of infrastructure has been defined for this: Critical Information Infrastructure (CII).

In this report, we review the definitions of CI and CII, review examples of regulatory approaches towards CII regulations in Asia Pacific, and identify specific principles and recommendations for a strong risk-based approach towards regulating CII.

In Summary:

### PRINCIPLE 1

A technologically neutral approach towards security standards is preferred for CII regulation, as technologies used by CII within their systems vary across sectors and each will require a differentiated security standards approach to protect different aspects of CII.

### PRINCIPLE 2

A risk-based, shared responsibility approach would be the most appropriate starting point for regulating CII.

### PRINCIPLE 3


A balance between voluntary and regulatory approaches using internationally-recognized standards and mutual recognition should be used for addressing risks to CII.

### PRINCIPLE 4

A harmonized and unified whole-of-government approach for CII regulations aligns cybersecurity requirements and enhances coordination and cooperation across sectors.

### PRINCIPLE 5

A close working relationship and regular dialogues between governments and industry allow for progressive and ongoing updates, assessment, and information sharing on the evolving threat landscape and technology offerings available for CII protection.



## 2. Critical Information and Infrastructure Regulations

As policymakers and regulators contemplate how to effectively regulate critical infrastructure amidst an evolving threat landscape, they need to consider how to define critical infrastructure, related assets, and the role of information communication technologies within critical infrastructure in today's digital world.

## 2.1 Definition – Critical Infrastructure (CI) and Critical Information Infrastructure (CII)

The motivation to protect CII has emerged in recent years as digital transformation and technology innovation continue to impact all sectors of industry.

### CI and CII

Critical infrastructure is “everything you don’t think about – the roads...the rigs and refinery...the electricity...the streetlights and lamps...”<sup>1</sup>

CI are the core and essential infrastructure and assets that a country needs to function and CII represent the ICT systems that underpin the operation of these CI. **CII are therefore the information infrastructure – from systems and software to technology hardware – that supports essential and, often, nationally significant services.**

### Defining Critical Infrastructure and Assets

There is no universal definition for CI as different countries have different key assets and critical systems they need to protect. However, there are some common sectors that have been identified. Countries should nevertheless be wary of overinclusive definitions of “critical infrastructure” and may consider how criticality methodologies (e.g., CISA’s methodology used in response to EO 13873<sup>2</sup>) can help target resources more effectively. Being overinclusive runs the risk that scarce resources are unnecessarily utilized to cover assets and systems which may not be as critical as other entities, while too broad a scope would make the ‘critical’ definition meaningless.

1 Bogost, I, 2003, The Atlantic, as quoted in Hayden, E., 2020, Critical Infrastructure Risk Assessment: The Definitive Threat Identification and Threat Reduction Handbook

2 CISA, Apr 2020, Executive Order 13873 Response Methodology For Assessing The Most Critical Information And Communications Technologies And Services [https://www.cisa.gov/sites/default/files/publications/ea-response-methodology-for-assessing-ict\\_v2\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/ea-response-methodology-for-assessing-ict_v2_508.pdf)

3 European Union Agency for Cybersecurity, n.d., Critical Infrastructures and Services <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii>

4 Cyber4Dev, 2022, Critical Information Infrastructure Protection (CIIP) <https://cyber4dev.eu/critical-information-infrastructure-protection-ciip/>

5 European Commission, 31 Mar 2011, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on Critical Information Infrastructure Protection ‘Achievements and next steps: towards global cyber-security’ /\* COM(2011) 163 final \*/ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0163:EN:HTML>

6 Cybersecurity and Infrastructure Security Agency, n.d., National Critical Functions Set <https://www.cisa.gov/national-critical-functions-set>

7 Cybersecurity and Infrastructure Security Agency, n.d., Critical Infrastructure Sectors <https://www.cisa.gov/critical-infrastructure-sectors>

The **European Council Directive 2008/114/EC** notes the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection: “ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.)”.<sup>3</sup>

Related, **Cyber4Dev EU**<sup>4</sup> defines CI as: “Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences”. Critical Infrastructure Protection is also defined as: “All activities aimed at ensuring the functionality, continuity and integrity of CI in order to deter, mitigate and neutralize a threat, risk or vulnerability.”

### Examples of CII Definitions

The EU’s CII Protection (CIIP) Plan is built on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation and criteria for European Critical Infrastructures in the field of ICT. It sets out the work to be done under each pillar by the Commission, the Member States and/or industry, with the support of the European Network and Information Security Agency (ENISA).<sup>5</sup>

The United States of America (USA)’s Cybersecurity and Infrastructure Security Agency (CISA)<sup>6</sup> defines “National Critical Functions” as a set of vital functions shared between the government and the private sector such “that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” These National Critical Functions have been classified<sup>7</sup> as 16 key infrastructure sectors: (1) chemical, (2) commercial facilities, (3) communications, (4) critical manufacturing, (5) dams, (6) defense industrial base, (7) emergency services, (8) energy, (9) financial services, (10) food and agriculture, (11) government facilities, (12) healthcare and public health, (13) information technology, (14) nuclear reactors, materials, and waste, (15) transportation systems, and (16) water and wastewater systems.

## A Transparent and Risk-based Approach

We recommend that governments practice transparency regarding how specific information operators serving CI are designated CII and what parts of the infrastructure are deemed critical for the purposes of regulation. In a digitally-enabled environment, the protection of CII includes both the protection of infrastructure as well as the establishment of policies required to protect digital infrastructure.

In some instances, countries also have cybersecurity regulations that specify definitions for CII.

For example, the **Singapore Cybersecurity Act 2018**<sup>8</sup> in Article 7, states that an entity is designated as CII by order of the Cybersecurity Commissioner where:

“(a) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and (b) the computer or computer system is located wholly or partly in Singapore.”

A total of 11 sectors have been identified as CII<sup>9</sup>: Aviation, Banking and Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security, and Emergency Services and Water.

At the same time, governments should adopt a risk-based approach when it comes to defining and regulating CII and put focus more on regulation for higher-risk and lighter measures where necessary to avoid over regulation.

**There is no universal definition for CI and by extension CII, although there may be commonalities. Governments' definitions for CI and CII should not be too broad to avoid becoming unmanageable and indistinguishable between what is critical and what is not. Governments should be transparent and adopt a risk-based approach to defining and regulating CII.**

### What are the Key Components Defining CII

Defining CII comprises of two main components:

- 1 The identification of essential assets, services, and functions by a state, usually via sectors.
- 2 The materiality and severity of the impact on the state in the event of a disruption of these sectors, in some cases considered the “severity of harm” that a disruption would have on the continued functioning of a state including on the level of confidence and well-being of citizens and the economy.

## 2.2 Regulations Protecting CI/CII in Asia Pacific

Across Asia Pacific, a number of approaches towards protection of CII have emerged. While many countries have expressed their concerns, every country is different and there is no one-size-fits-all approach. As examples, we look at the different approaches taken by three Asia Pacific countries, Singapore, Australia, and Japan.

### 2.2.1 Singapore Cybersecurity Act 2018 Review and Update to the Cybersecurity Code of Practice for CII

In Singapore, the approach towards CII is driven by the Cyber Security Agency of Singapore (CSA). The Cybersecurity Act 2018<sup>10</sup> regulates CII insofar as they are delivering “essential services in the physical world such as water and power”. The update of the Cybersecurity Code of Practice for CII in 2022 broadens this approach to cover CII with the justification that CII falls under the remit of cybersecurity to “improve awareness of threats over Singapore’s cyberspace, protect virtual assets (e.g. systems hosted on the cloud) as CII if they support essential services.”<sup>11</sup> The rationale<sup>12</sup> for the update to the Act was threefold:

- To help CII improve their odds of defending against cyber threat actors using sophisticated threats;
- To allow CII to be more agile to respond to emerging risks in specific domains; and
- To enhance coordinated defenses between Government and private sectors to identify, discover and respond to cyber threats and/or attacks in a timely manner.

#### Observations

**The need for local response teams may not be the most efficient approach for security of CII assets.** Rather than adopting a blanket approach for all sectors to require locally present representatives to be accountable and responsive to a regulator, the approach should be calibrated based on the risk. Discussions with CII representation and industry is important to help determine the most effective options.

8 Singapore Cybersecurity Act, 2018 <https://sso.agc.gov.sg/Act/CA2018>

9 Cyber Security Agency of Singapore, 4 Mar 2022, Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CII <https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis>

10 Singapore Cybersecurity Act, 2018 <https://sso.agc.gov.sg/Act/CA2018>

11 Cyber Security Agency of Singapore, 4 Mar 2022, Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CII <https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis>

12 Cyber Security Agency of Singapore, 4 Mar 2022, Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CII <https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis>

## Australia Security of Critical Infrastructure Act 2018

In Australia, CII regulations are driven primarily by the Cyber and Infrastructure Security Centre (CISC), which is part of the Australia Department of Home Affairs.<sup>13</sup> CII regulations are espoused within three legislations:

- Security of Critical Infrastructure Act 2018<sup>14</sup>, together with
- Security Legislation Amendment (Critical Infrastructure) Act 2021<sup>15</sup>, and
- Security Legislation Amendment (Critical Infrastructure Protection) Act 2022<sup>16</sup>

### Observations

**1. Transparent and consultative process.** CCAPAC notes that Australia has adopted a transparent, risk-based approach towards classifying CI<sup>17</sup>, with online artifacts and references such as a Risk Management Program factsheet<sup>18</sup> published by the CISC to increase public education and awareness of how to implement a risk management program for Australia's critical infrastructure. Australia's consultative process increases this public-private engagement process, and the transparency on criteria used to select and identify CII provides clarity to the industry on which sectors and services are classified – and therefore regulated – as CII.

**2. Follows best practices in cybersecurity with strong use of internationally-recognized standards.** CCAPAC notes also that Australia's CII regulations are largely supportive of and reference internationally-recognized standards such as ISO/IEC 27001, the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST), and other equivalent frameworks.<sup>19</sup>

**3. Mandatory incident reporting afford government agencies visibility of the country's cyber threat landscape, but at the expense of incident investigation.** Sharing of threat information quickly and efficiently with key stakeholders is important to help others defend against threats. Whilst incident reporting keeps government agencies aware of the threats, it is at the expense of investigating and uncovering actionable intelligence as soon as possible, such as the attack mechanism, signatures, command, and control domains used, etc, which are needed by stakeholders to defend themselves. These investigative resources are scarce and costly, making it hard to simply add resources. The impact is especially acute with shorter reporting timeframes.



**a. Recommendation:** Threat intelligence sharing leveraging common standards like STIX/TAXII enables automation and speed. It provides a way that does not expose sensitive information, thereby avoiding the need for legal purview beyond the initial sharing agreement and permitting security teams to have more freedom to share. It should be the primary means for short timeframe updates. This can be complemented with more comprehensive regulatory reports with longer timeframes for critical incidents.

**4. Reporting regulations are onerous and may increase compliance costs.** In the first instance, Australia's risk management program includes annual reporting requirements, which will increase compliance costs and may be considered overly-onerous.



**a. Recommendation:** It may be useful to consider where reporting requirements may be reduced, and/or replaced with standardized international audit report submissions.

**5. In some instances, regulatory requirements may undermine the cybersecurity they are hoping to achieve.** Provisions requiring CII providers to include backdoors, insert software into systems for monitoring, or creating decryption capabilities, may not necessarily be best practice for CII, as this may introduce vulnerabilities. The Assistance and Access Act is focused instead on how law enforcement and intelligence agencies may seek assistance and work closely with industry. However, Australia's CII regulations which grant the government assistance measures make reference to/cover many digital services such as the "data storage or processing sector", although that is limited to business critical data.

13 Australia Cyber and Infrastructure Security Centre - Department of Home Affairs, 24 Jun 2022, Legislative information and reforms – Critical Infrastructure <https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure>

14 Australia Security of Critical Infrastructure Act, 2018 <https://www.legislation.gov.au/Details/C2021C00570>

15 Australia Security Legislation Amendment (Critical Infrastructure) Bill, 2021, [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bId=r6657](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657)

16 Australia Security Legislation Amendment (Critical Infrastructure Protection) Bill, 2022, [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bId=r6833](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6833)

17 Australia Critical Information Centre, n.d., Risk Assessments <https://www.homeaffairs.gov.au/nat-security/files/cic-factsheet-risk-assessments.pdf>

18 Cyber and Infrastructure Security Centre, Aug 2022, Risk Management Program <https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cisc-factsheet-risk-management-program.pdf>

19 Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022, <https://www.homeaffairs.gov.au/reports-and-pubs/files/soci-rmp-rules-legislative-instrument-lin-22-018.PDF>



## 2.2.3 Japan's Cybersecurity Policy for Critical Infrastructure Protection 2022

Japan's CII protection has been driven by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), through the Japan Cybersecurity Policy for Critical Infrastructure Protection 2022. Under a proposed National Security Strategy of Japan<sup>20</sup>, it was recognized that to ensure secure and stable use of cyberspace, there is a need to further strengthen cybersecurity capabilities in Japan and respond to emerging cyber threats. As such, the NISC is expected to be restructured to establish a new organization to comprehensively coordinate policies in a centralized manner, with further work on legislation to strengthen cybersecurity efforts, and coordination with other related policies such as economic security and enhancement of technical capabilities related to national security.

The current NISC 2022 policy contains a non-mandatory common action plan shared between the government and CI operators. This action plan delineates two parties with interdependent responsibilities to CI protection:

- Government bears responsibility for promoting independent measures by CI operators relating to CI cybersecurity and implementing other necessary measures as it deems fit, and
- CI operators independently carry out relevant protective measures related to cybersecurity.

The policy self-identifies as "risk-based" (Section 4), and identifies 14 sectors as critical infrastructure, alongside applicable CI operators, and CI information system examples in Annex 1 (see table below). The 14 sectors are: (1) Information and communication services, (2) Financial services, including banking services, life insurance services, general insurance, securities services, (3) Aviation services, (4) Airport, (5) Railway services, (6) Electric power supply services, (7) Gas supply services, (8) Government and administrative services, (9) Medical services, (10) Water services, (11) Logistic services, (12) Chemical industries, (13) Credit card services, and (14) Petroleum industries.

The policy sets out examples of CI service outage examples, and expects stakeholders to undertake defined actions along five measures:

- 1 Enhancement of Incident Response Capability**
- 2 Maintenance and Promotion of the Safety Principles**
- 3 Enhancement of Information Sharing System**
- 4 Utilization of Risk Management**
- 5 Enhancement of the Basis for the Critical Infrastructure Protection**

### Observations

**Nationally-coherent approach towards national and CI/CII security.** Japan's Cybersecurity for Critical Infrastructure Protection is a part of the Japan Cybersecurity Policy for Critical Infrastructure Protection (2022)<sup>21</sup>. Countries should follow this best practice as regulatory alignment within the country on CI and CII policy reduces uncertainty.

CI sectors	Applicable CI operators	Applicable critical information system examples
Information and communications services	<ul style="list-style-type: none"> <li>• Major electronic communications operators</li> <li>• Major terrestrial base broadcast operators</li> <li>• Major cable television operators</li> </ul>	<ul style="list-style-type: none"> <li>• Network systems</li> <li>• Operation support systems</li> <li>• Organization/operation systems</li> </ul>
<b>Financial Services</b> <ul style="list-style-type: none"> <li>• Banking services</li> <li>• Life insurance services</li> <li>• General insurance</li> <li>• Securities services</li> <li>• Fund settlement services</li> </ul>	<ul style="list-style-type: none"> <li>• Banks, credit unions, labor credit unions, agricultural cooperatives, etc</li> <li>• Financial settlement agencies</li> <li>• Electronic credit record agencies</li> <li>• Life insurance services</li> <li>• General insurance services</li> <li>• Securities firms</li> <li>• Financial product exchanges</li> <li>• Money transfer agencies</li> <li>• Financial product clearing agencies etc.</li> <li>• Major fund transfer businesses</li> <li>• Major prepaid payment instruments (third-party issuer) etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Accounting systems</li> <li>• Financial securities systems</li> <li>• International systems</li> <li>• External connection systems</li> <li>• Financial institution internet work systems</li> <li>• Electronic credit record agency systems</li> <li>• Insurance services systems</li> <li>• Securities trading systems</li> <li>• Exchange systems</li> <li>• Money transfer systems</li> <li>• Clearance systems etc</li> </ul>
Aviation services	<ul style="list-style-type: none"> <li>• Major scheduled air transport operators</li> </ul>	<ul style="list-style-type: none"> <li>• Flight systems</li> <li>• Reservation/boarding systems</li> <li>• Maintenance systems</li> <li>• Cargo systems</li> </ul>
Airport	<ul style="list-style-type: none"> <li>• Major airport and airport building operators</li> </ul>	<ul style="list-style-type: none"> <li>• Vigilance, guard and monitoring systems</li> <li>• Flight information systems</li> <li>• Baggage handling systems</li> </ul>
Railway services	<ul style="list-style-type: none"> <li>• Major railway operators including JR companies and major private railway companies</li> </ul>	<ul style="list-style-type: none"> <li>• Railway traffic control systems</li> <li>• Power supply control systems</li> <li>• Seat reservation system</li> </ul>
Electric power supply services	<ul style="list-style-type: none"> <li>• General electric power transmission and distribution operators and major power producers, etc</li> </ul>	<ul style="list-style-type: none"> <li>• Electric power control systems</li> <li>• Smart meter systems</li> </ul>
Gas supply services	<ul style="list-style-type: none"> <li>• Major gas supply operators</li> </ul>	<ul style="list-style-type: none"> <li>• Plant control systems</li> <li>• Remote monitoring and control systems</li> </ul>
Government and administrative services	<ul style="list-style-type: none"> <li>• Local governments</li> </ul>	<ul style="list-style-type: none"> <li>• Local government information systems</li> </ul>
Medical services	<ul style="list-style-type: none"> <li>• Medical facilities (excluding small-scale facilities)</li> </ul>	<ul style="list-style-type: none"> <li>• Medical examination record management systems, etc.</li> <li>• Medical examination support systems</li> <li>• Community medical care support systems</li> </ul>
Water services	<ul style="list-style-type: none"> <li>• Water service operators and city water service providers (excluding small-scale facilities)</li> </ul>	<ul style="list-style-type: none"> <li>• Water utility and water supply monitoring systems</li> <li>• Water utility control systems, etc.</li> </ul>
Logistics services	<ul style="list-style-type: none"> <li>• Major logistics operators</li> </ul>	<ul style="list-style-type: none"> <li>• Collection and delivery management systems</li> <li>• Cargo tracking systems</li> <li>• Warehouse management systems</li> </ul>
Chemical industries	<ul style="list-style-type: none"> <li>• Major petrochemical facilities</li> </ul>	<ul style="list-style-type: none"> <li>• Plant control systems</li> </ul>
Credit card services	<ul style="list-style-type: none"> <li>• Major credit card services operators</li> <li>• Major settlement agencies</li> <li>• Designated credit information agencies etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Credit card payment-related systems (intermediation of comprehensive credit card purchases and intermediation of two-month installment purchases)</li> <li>• Credit information provision and collection systems</li> </ul>
Petroleum industries	<ul style="list-style-type: none"> <li>• Major petroleum refinery facilities and petroleum wholesalers</li> </ul>	<ul style="list-style-type: none"> <li>• Sales order management system</li> <li>• Product management system</li> <li>• Shipping management system etc</li> </ul>

**Note 1** The operators listed here are CI operators for which measures should be implemented on a priority basis, and review of the applicable operators is to be carried out based on changes in the business environment and progressive dependence on IT, when the Cybersecurity Policy is revised. Source: Japan Cybersecurity Policy for Critical Infrastructure Protection<sup>22</sup>

**Note 2** The operators listed here are examples and do not constitute a comprehensive list.

<sup>20</sup> <https://www.cas.go.jp/jp/siryuu/221216anzenhoshou/nss-e.pdf>

<sup>21</sup> National Center of Incident Readiness and Strategy for Cybersecurity (NISC), 2018, Japan Cybersecurity Policy for Critical Infrastructure Protection 2022 [https://www.nisc.go.jp/eng/pdf/cs\\_policy\\_cip\\_eng\\_v4.pdf](https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf)

<sup>22</sup> Japan Cybersecurity Policy for Critical Infrastructure Protection, 17 Jun 2022 [https://www.nisc.go.jp/eng/pdf/cip\\_policy\\_2022\\_eng.pdf](https://www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf)





# 3. Principles for Approaching Critical Information Infrastructure Regulations Proportionately

This chapter draws from the different approaches taken by various Asia Pacific governments in regulating CII and uses them to propose a general principled framework by which CII regulations may be considered for (1) improving on existing regulations and legislation, and (2) putting in place CII regulations where none currently exist.

## PRINCIPLE

# 1

**A technologically-neutral, “right-solutions for the right fit” approach towards security standards is preferred for CII regulation, as technologies used by CII within their systems are different for separate sectors, and each will require a differentiated security standards approach to protect different aspects of CII.**

An observation of the different sectors involved with CI and CII reveals that there will likely be vastly different types of information systems supporting the various critical sectors. **A technology neutral approach towards security standards would therefore be preferred for CII regulation, as technologies used by CII are different for separate sectors, and each will require a differentiated security standards approach to protect different aspects of CII.** Furthermore, a technology neutral approach allows regulators to be more outcome focused, which allows for greater flexibility in response to the constantly evolving technology and risk landscape.

For example, in the USA, the CI sectors are vast and/or specialized, and delineating security standards for each would likely result in CII regulations which are too sector-specific and may be difficult to keep updated.

Similarly in Singapore<sup>23</sup>, delineating cybersecurity protection for each and every one of designated CI may be too sector-specific. It may be more useful to identify practices which are technologically-neutral, and relevant to the same/similar high-level infrastructure (such as broad data services) which support both CI and non-CI entities. Singapore's update to its Cybersecurity Code of Practice for Critical Information Infrastructure 2.0 largely adopts a technology neutral and outcome focused approach without prescribing any specific technology or application except for the use of Domain Name System Security Extension (DNSSEC) for CII assets with Internet-facing Domain Name System (DNS) servers.<sup>24</sup>

Rather than specify a technological response to the cyber threat, it is more useful to focus on the fact that “response efforts may be driven by first responders, owners/operators, or regional and federal resources, but responsibility for recovery in a predominately voluntary system, such as in the U.S., generally falls to the owners and operators who know the infrastructure best.”<sup>25</sup>

CCAPAC notes that cybersecurity regulators and policymakers should adopt a technologically neutral approach to regulating CII instead of formulating prescriptive one-size-fits-all frameworks that may not be accurate, and/or impractical to implement, and/or costly to put in place.

<sup>23</sup> Cyber Security Agency of Singapore, 4 Mar 2022, Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs <https://www.csa.gov.sg/News/Press-Releases/review-of-the-cybersecurity-act-and-update-to-the-cybersecurity-code-of-practice-for-ciis>

<sup>24</sup> Cybersecurity Agency of Singapore, 4 July 2022, Cybersecurity Code of Practice for Critical Information Infrastructure, Second Edition, [https://www.csa.gov.sg/-/media/Csa/Documents/Legislation\\_COP/CCoP\\_Second-Edition.pdf](https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_COP/CCoP_Second-Edition.pdf)

<sup>25</sup> Cybersecurity and Infrastructure Security Agency, Nov 2019, A Guide to Critical Infrastructure Security and Resilience <https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf>

## PRINCIPLE 2

**A risk-based, shared responsibility approach would be the most appropriate starting point for regulating CII.**

While some sectoral-level regulations may exist, the overall approach towards CII protection should be risk-based, where government policy regulates CII based on the size of the risk and materiality of the impact that an adverse event would have on the CI sector. A good place to start understanding a risk-based approach would be the CISA guidelines:

“ Not all infrastructure within an industry sector is critical to a nation or region. It is necessary to identify which infrastructure is both critical to maintain continued services or functions and vulnerable to some type of threat or hazard. Prioritizing the allocation of available resources to that subset of infrastructure can enhance a nation's security, increase resiliency, and reduce risk.<sup>26</sup> ”

Japan's Cybersecurity Policy for Critical Infrastructure Protection (CIP) 2022<sup>27</sup> promotes such use of risk management in critical infrastructure services (CIS):

“ Risk management activities are necessary in order to make a systematic response to risks that disrupt the continual provision of CISs, which is the purpose of CIP... stakeholders shall utilize risk management appropriately... In a situation in which risks relating to CISs are changing dynamically, including recent environmental changes and technological innovations, etc., in order to deal accurately with risks and bring them within acceptable limits, the involvement of top management is critically important. To this end it is important for organizations to properly recognize the impact that any suspension of the continual provision of CISs would have on management of their operations, and foster awareness of the need to make organization-wide efforts, visualizing this awareness through the promotion, monitoring and measurement of continual activities, and making improvements accordingly. ”



Japan provides further information on how to promote risk management in Section 4.1 Promotion of risk management:

“ In order to accurately tackle risk management initiatives CI operators must understand the characteristics (profile) of their own organization, and also engage in repeated Plan-Do-Check-Act (PDCA) cycles and promote continual activities (processes) to ensure CIP policies optimized to individual organizations. In particular, it is clear that advances in digital transformation will significantly change the environment surrounding CI and associated risks in the future, and therefore in order to effectively implement continual improvements while ensuring continual provision of CISs, it is necessary for CI operators to understand the risks their organizations are facing and their degree of severity, and initiate new improvements by starting to clarify the characteristics (profile) of their organization's CISs. ”

<sup>26</sup> Cybersecurity and Infrastructure Security Agency, Nov 2019, A Guide to Critical Infrastructure Security and Resilience <https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf>

<sup>27</sup> The Cybersecurity Policy for Critical Infrastructure Protection, 17 Jun 2022 [https://www.nisc.go.jp/eng/pdf/cip\\_policy\\_2022\\_eng.pdf](https://www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf)

This brings up another aspect of CII regulations – CI are the nationally-identified infrastructure to be protected, while CII may be the same infrastructure, and/or specific services which have been appointed to serve these CI via service agreements. This outsourced approach makes necessary a shared responsibility model for CI and CII protection: **CI operators should conduct a risk assessment of their critical business operations (both the threat and the possible adverse impact it may have), share this with their information infrastructure provider (thus the CII), and together this informs the assessment of how to protect the CI by protecting and supporting the CII services, and their corresponding risk profiles.**

- An example would be power operators (CI) have a public website (hosted on an information system), with a different risk profile to billing systems, which in turn have a different risk profile to operational power generation systems.
- CCAPAC notes that while recognizing that governments should always have the discretion to decide, there should be some flexibility to allow for service providers to assess the risks and allow them to use other innovative products for low-sensitive or non-critical services.

Similarly, governments should consider more proportionate approaches (for example having different levels of classification) to different systems and the functions they are meant for.

- For example, having onerous requirements for less critical services such as videoconferencing tools, collaboration tools, public websites, may not be as necessary as opposed to systems used for critical functions such as supervisory control and data acquisition (SCADA) systems, etc.

CCAPAC believes that a risk-based model allows governments to “step up, don’t step in” – that in the case of a risk assessment, governments can provide support through actionable intelligence and technical assistance during critical incidents, but not step in to take command.

**CCAPAC recommends the use of internationally recognized standards for establishing strong cybersecurity control mechanisms for protecting CII.** As identified in Principle #3, CCAPAC recommends adopting and implementing internationally-recognized standards and best practices for cybersecurity, as we believe this is the most appropriate way to protect national CII efficiently, effectively, and in a way that is interoperable with other jurisdictions. One risk-based model for Asia Pacific governments to consider following is the US CISA model, Executing a CI Risk Management Approach.<sup>28</sup>

The use of internationally recognized standards as a cybersecurity control mechanism for CII also helps to reduce confusion and complexity on adoption of technology solutions, and accelerate implementation.

CCAPAC also recommends taking a measured approach towards reporting cybersecurity incidents. Any form of incident reporting should be risk-based and appropriately scoped to avoid overwhelming regulators and overburdening security operations teams. CII service providers should report incidents to the CII, who in turn will assess whether they have an obligation to report incidents to the regulator. Requiring CII service providers to report directly to regulators could potentially put them in an untenable position of having to choose between complying with a regulatory requirement and violating contractual requirements with their CII customers.

Reporting obligations should distinguish between (a) an interruption or disruption of services provided to CII, and (b) a security incident that could potentially impact CII, including impacting the broader public and business community. In (a), the CII can either report the incident or direct its service provider to report to the regulator. For (b), the reporting requirement from CII service providers should be to provide information to the CII with the purpose of helping the CII understand whether there is a reporting obligation. CII service providers should not pre-judge what should require reporting as it puts them in a position of conflict of interest with their CII customer.

In terms of reporting timeline, regulators should ensure that there is sufficient amount of time to ensure a proper investigation can be conducted. Reporting requirements should also set clear minimum thresholds. A well-constructed incident reporting requirement is able to recognize that only certain entities present sufficient systemic risk and thus require mandatory reporting. Even for such entities, there should be a clear delineation between potential, suspected, or threatened incidents and incidents that cause actual and significant harm. Upon assessment that these thresholds have been met, a reasonable amount of time should be given to gather the relevant information to file a report.

28 Cybersecurity and Infrastructure Security Agency, Nov 2019, A Guide to Critical Infrastructure Security and Resilience <https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf>



**PRINCIPLE  
3**

**A balance between voluntary and regulatory approaches using international standards and mutual recognition should be used for addressing risks to CII.**

Following on with the principles of a risk-based, technologically-neutral approach towards CII, governments should seek to balance between voluntary and regulatory approaches to address risks to CII. Beyond the regulatory/legislative approaches covered earlier in this paper, CCAPAC believes that governments should implement guardrails, not roadblocks, to better CII security.

Governments should adopt approaches that are aligned with the use of widely adopted internationally-recognized standards and with mutual recognition of industry standards. The approach should be a sensible and meaningful threshold for CII risk management which balances the need for security, business efficiency, and innovation. Countries should encourage CII organizations to leverage internationally-recognized risk management frameworks to identify, manage, and communicate risk effectively across diverse partners.

#### Some examples include:

- NIST Cybersecurity Framework which is a sector-agnostic voluntary framework that offers guidance on standards, guidelines, and best practices to manage cybersecurity risk.
- Certifications such as Common Criteria that offer assurance that products have been evaluated and certified based on the ISO/IEC 15408 standard for computer security.
- France (ANSSI), for example, has a very rigorous and unique approach for evaluating and certifying network equipment that will run in CI environments – and if a service provider is certified under ANSSI's strict regime, mutual recognition of adequacy may be an approach to allow for addressing CII risk (borrowing a term and the concept from the European Union (EU) General Data Protection Regulation (GDPR)).

These internationally-recognized frameworks enable and incentivize CII organizations to adapt as threats and technologies evolve over time.

The benefits of taking the approach to strike a balance between voluntary and regulatory approaches (depending on criticality and risk) include:

**1. Specificity.** The ability to enable sector-specific matching of CI sector with the relevant technical specification and standard required for best securing the CII. E.g., Cloud Service Providers (CSPs) would tend to have greater redundancy in infrastructure and competence in cyber capabilities, and hence, voluntary programs would work best for such a sector.

**2. Responsiveness.** As new technology, new cyber threats and adversary behavior, new cybersecurity strategies, and new business models constantly evolve, any regulatory requirements on CII will demand constant revision towards technology risk management approaches. This places a heavy policy revision and consultation load on governments to ensure policy is always updated and responsive to new cyber threats. Some examples where this has been observed:

- Australia established a cloud services accreditation process for government technology vendors under the Australian Signals Directorate (ASD). However, following independent reviews demonstrating that this shut out smaller players from participating in government tenders (as well as being slow and providing low security assurance), the Cloud Services Certification Program (CSCP) was abolished in 2020<sup>29</sup> for an alternative approach that sets up a whole of government Cloud Computing Security Considerations.<sup>30</sup> This approach establishes risk management principles, and runs in tandem with the Australian Information Security Manual, which is updated every 6 months.<sup>31</sup>
- In 2022, the Singapore Cyber Security Agency updated the Singapore Cybersecurity Act 2018 and the Cybersecurity Code of Practice for CII,<sup>32</sup> which were introduced to complement the Singapore Computer Misuse Act that was established in 1993. The Computer Misuse Act has been reviewed 8 times since 1993 at an average interval of 3.5 years. These dates show the regularity of policy review phases to ensure Singapore stays up to date with the ever evolving technology and threat landscape.
- Similarly, following a two-year review process that started in 2018, Bank Negara Malaysia released their Risk Management in Technology (RMiT) policy on 19 Jun 2020.<sup>33</sup>
- The Japan ISMAP cloud certification<sup>34</sup> is an example of not being able to keep up with its own regulation-imposed renewal cycles. ISMAP requires an annual evaluation; however the process takes time, and existing certifications tend to expire before the Japanese government can issue new certificates.

CCAPAC recommends striking a balance between developing a voluntary standards-based approach and regulation, as this will (1) allow for greater flexibility and responsiveness when needing to update CII requirements to address the constantly-evolving threat environment, and (2) allow for best-in-class infrastructure and competence in specific sectors to be deployed where they are best suited e.g., CSPs would have better competencies and redundancy in infrastructure and competence in cyber capabilities.

29 ZDnet, 2 Mar 2020, Australian government's certified cloud list to expire come June 30  
<https://www.zdnet.com/article/australian-governments-certified-cloud-list-to-expire-come-june-30/>, Australian Signals Directorate, 2 Mar 2020, Cloud Services  
<https://www.cyber.gov.au/acsc/view-all-content/programs/irap/asd-certified-cloud-services>

30 Australian Cyber Security Centre, n.d., Cloud Computing Security Considerations  
<https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>

31 Australian Cyber Security Centre, n.d., Cloud Computing Security Considerations  
<https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>

32 Australian Cyber Security Centre, n.d., Cloud Computing Security Considerations  
<https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>

33 Australian Cyber Security Centre, n.d., Cloud Computing Security Considerations  
<https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>

34 Please find the source and cite

**PRINCIPLE**  
**4**

**A harmonized and unified whole-of-government approach for CII regulations will align cybersecurity requirements and enhance coordination and cooperation across sectors**

En route to a whole-of-government approach towards CII regulations (see the Japan example in previous chapter), a number of countries' sectoral regulators for some CI have taken steps to put in place guidelines and frameworks by which technology is being deployed within their sectors. This is particularly within tightly-regulated sectors, such as the financial services industry.

There will be a need to work with sectoral regulators to ensure there is regulatory harmony within each country's CII regulations, particularly if the sectoral regulation pre-dates the CII regulation.

For example, in Asia Pacific (and across the world), the financial services industry is regulated by the relevant financial authority and/or central bank, such as the Australian Prudential Regulation Authority (APRA)<sup>35</sup> Japan's Financial Services Agency (FSA),<sup>36</sup> the Monetary Authority of Singapore (MAS),<sup>37</sup> Bank Negara Malaysia (BNM),<sup>38</sup> etc.

- APRA – CPS 220 and CPG 220 on Risk Management<sup>39</sup>
- Japan FSA - FSA publishes an English translation of Principles for Model Risk Management<sup>40</sup>
- MAS – Guidelines on Risk Management Practices – Technology Risk<sup>41</sup>
- Malaysia BNM - Risk Management in Technology (RMiT)<sup>42</sup>

To manage these cybersecurity requirements domestically, a central coordinating mechanism is essential to align requirements at the national and sectoral level to ensure there are no overlaps or conflicting requirements which may complicate compliance. Some countries have established a separate cybersecurity regulator or designated an existing agency to oversee domestic cybersecurity and lead the discussion on regulatory harmonization.

CCAPAC notes that sectoral agencies tend to develop a risk-based approach towards general technology outsourcing, rather than developing specific CII-focused regulations. Therefore, if there is a national-level CII regulation, these sectoral regulatory approaches will need to be integrated and harmonized with the national level regulation. An alternative approach is also possible – a national-level regulation could use the existing sector-specific regulations to build out a national-level CII regulation. This coordination and harmonization can be performed through a dedicated agency with the mandate and resources to oversee cybersecurity at a national level, including endorsing the use of internationally-recognized standards for cross-border harmonization.

35 Australian Prudential Regulation Authority <https://www.apra.gov.au>

36 Japan Financial Services Agency <https://www.fsa.go.jp/en/>

37 Monetary Authority of Singapore <https://www.mas.gov.sg/>

38 Bank Negara Malaysia <https://www.bnm.gov.my/>

39 Australian Prudential Regulation Authority, n.d., Risk Management <https://www.apra.gov.au/risk-management>

40 Japan Financial Services Agency, 12 Nov 2021, FSA publishes an English translation of Principles for Model Risk Management <https://www.fsa.go.jp/en/news/2021/2021112en.html>

41 Monetary Authority of Singapore, 18 Jan 2021, Guidelines on Risk Management Practices – Technology Risk <https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines>

42 Bank Negara Malaysia, 19 Jun 2020, Risk Management in IT [https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+\(RMiT\).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078](https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078)

## PRINCIPLE 5

**A close working relationship and regular dialogues with industry allows for progressive and ongoing updates, assessment, and information sharing on the evolving threat landscape and technology offerings available for CII protection.**

Following the previous principle, CCAPAC recommends going beyond just engaging specific government regulators, but also working closely with the technology industry and CII owners to better balance between government concerns on national security and implementing proportional risk-based and process-based solutions. We also encourage engagement between CII owners and vendors.

This is important to establish information sharing on the evolving cyber threat landscape between the public and private sector, and also for governments to capitalize on best-of-class technology developments and information security cyber protections which the private sector market may be leading in.

This public-private partnership dialogue model is particularly important in countries where the private sector owns and/or operates significant portions of CI. As CII functions increasingly rely on connected technology – and given the dynamic and evolving nature of cybersecurity threats and the technologies and practices used to address them – countries should avoid prescriptive, compliance-based approaches to manage CII risk.

One example of how regular public private dialogues have been established are the Information Sharing and Analysis Centers (ISAC), which collect, analyze, disseminate information on vulnerabilities, threats, and intrusions by collaborating with the government.<sup>43</sup>

Another approach is public private partnership which is useful for the government to consider facilitating emergency preparedness planning among CII with interdependencies, including developing playbooks, hosting tabletop exercises, etc. Governments should explore opportunities to serve as a convener of stakeholders with CII interdependencies and provide protection/opportunities for those stakeholders to prepare/respond to cyber incidents.

CISA hosts cross-sector working groups such as the Tri-Sector Working Group, which includes representatives from the Communications Sector, Financial Services Sector, and Electric Sub-Sector, to identify and address risk related to their interdependencies.

Similarly, the U.S. government convened stakeholders throughout the COVID-19 pandemic to identify and address risks to CI sectors due to the shortage of semiconductors, personal protective equipment (PPE), and to identify/help prioritize the availability of essential workers.

<sup>43</sup> CSO 26 Jul 2022, What is an ISAC or ISAO? How these cyber threat information sharing organizations improve security <https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html>



# 4. Summary

## Recommendations for Approaching Critical Information Infrastructure Management

CCAPAC supports strong security for CII, and we are aligned with governments and regulators on ensuring CII are secure, resilient, and where risk is managed proportionately. We are keen on working closely and collaborating with the government on meeting this shared objective in the most effective and efficient manner possible.

Following this review of CII regulations and guidelines in Asia Pacific, in summary:

- **Principle #1**  
A technologically neutral approach towards security standards is preferred for CII regulation, as technologies used by CII within their systems are different for separate sectors, and each will require a differentiated security standards approach to protect different aspects of CII.
- **Principle #2**  
A risk-based, shared responsibility approach would be the most appropriate starting point for regulating CII.
- **Principle #3**  
A balance between voluntary and regulatory approaches using international standards and mutual recognition should be used for addressing risks to CII.
- **Principle #4**  
A harmonized and unified whole-of-government approach for CII regulations aligns cybersecurity requirements and enhances coordination and cooperation across sectors.
- **Principle #5**  
A close working relationship and regular dialogues between governments and industry allow for progressive and ongoing updates, assessment, and information sharing on the evolving threat landscape and technology offerings available for CII protection.



# 5. Critical Information Infrastructure Considerations Checklist

## Defining and governing CII

- Clear and updated definitions of critical information and critical information infrastructure which are technology neutral, and outcome focused
- Legislation and regulations which govern the protection of critical information infrastructure which includes voluntary and mandatory requirements
- Leverage and encourage the use of internationally recognized standards, best practises, and mutual recognition of industry standards and certifications

## Coordinating with stakeholders

- Domestic coordination with sectoral regulators to align definitions and harmonize regulatory requirements
- Regular public consultations with industry, civil society, and other relevant stakeholders on:
  - Definitions of CI and CII
  - Using a risk-based approach
  - Transparency of the approach
- International coordination with regulators from other jurisdictions to align reporting requirements and templates

## Information sharing and education

- Voluntary information sharing schemes to encourage cooperation between public and private sector





The Coalition for Cybersecurity in Asia-Pacific or CCAPAC is a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building.

<https://ccapac.asia>