Critical Information Infrastructure and Supply Chain Security

A risk-based approach towards ensuring supply chain resilience

https://ccapac.asia

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. To find out more on how to join us, visit our website at https://ccapac.asia

Table of Contents

Chapter 1
Executive Summary

In recent years, concerns regarding supply chain risks have intensified among policymakers in the Asia-Pacific (APAC). These risks have become even more apparent as global events have disrupted critical supply chains, negatively affecting not only the economy but society as well.

The Coalition for Cybersecurity in Asia Pacific (CCAPAC)[1] notes that while the global integration of supply chains has created new efficiencies, it has also introduced higher levels of third-party dependency risks, which is particularly significant for managing critical information infrastructure (CII).

To assist policymakers on how to create effective policies for supply chain resilience, this paper reviews the key principles behind supply chain risk management (SCRM), particularly as it pertains to CII and its management. It reviews key country approaches towards CII and SCRM, and identifies four key commonalities in APAC regulatory approaches:

1. Prioritizing Critical Infrastructure (CI) and Building on Existing CI Regulatory Regimes;
2. Establishing Guidelines for Identifying, Assessing, and Managing Supply Chain Risks;
3. Facilitating Education, Training, and Information-sharing;
4. Supporting International Collaboration and Capacity Building.

The paper reviews various measures and mechanisms to enhance supply chain resilience, drawing from internationally-recognized best practices, standards, and technical mechanisms to ensure a risk-based and process-based approach. This technical review focuses on four hierarchical levels where SCRM CII policy may be applied: at the (1) infrastructure-level, (2) entity-level, (3) national- and sector-level, and (4) global- and regional-level.

This paper concludes with a call to action with four recommendations to enhance the security of supply chains in APAC markets for CII:

Recommendation **#1:**
Foster Resilience through Public-Private Collaboration

Recommendation **#2:**
Encourage Innovation and Experimentation

Recommendation **#3:**
Take a Comprehensive Approach to Strengthen Infrastructure Resilience

Recommendation **#4:**
Promote Regional Cooperation and Joint Capacity Building

CCAPAC is committed to positively shaping the cybersecurity environment in APAC, and we welcome comments on this report and discussions with governments and cybersecurity agencies to further strengthen and develop a strong and secure ecosystem in APAC.

Chapter 2
Principles of Supply Chain Risk Management (SCRM) – An Overview of Regulatory Approaches in APAC

2.1 Rising Concerns about Supply Chain Risks

In recent years, concerns regarding supply chain risks have intensified amongst policymakers in the Asia-Pacific (APAC). These risks have become even more apparent as global events have disrupted critical supply chains, negatively affecting not only the economy but society as well.

The total cost of supply chain disruptions in the US and Europe in 2020 is estimated to amount to USD 4 trillion.[2]

- One key challenge that countries have faced is the global semiconductor shortage,[3] which has not only slowed down production and increased costs across diverse industries ranging from electronics, to healthcare, and aerospace, but has also affected critical industries with national security implications, including defense and communications. Intensifying US-China tensions and the COVID-19 crisis have created demand-supply constraints with follow-on consequences on Japanese, Korean, Dutch, and US companies located along various parts of the supply chain.[4]

- Another challenge to supply chains is the Russian-Ukraine war, where heavy sanctions on the Russian economy has led to rising global energy prices and aggravated energy shortages,[5] which has in turn disrupted supply chains across a range of export markets.

In addition to direct supply chain disruptions, cyberattacks on supply chains have increased in the last few years. A 2023 study estimates the cost of cyberattacks on supply chains to be about USD 4.35 million per incident.[6]

We therefore see that the global integration of supply chains has created new efficiencies, but also introduced higher levels of third-party dependency risks. Further, the digitalization of supply chains has made them more complex, interconnected, and interdependent than before. In fact, 97% of APAC respondents in a 2022 survey on supply chain cyber risk management highlight that they have been negatively impacted by a cyber security breach in their supply chain.[7]

2.2 Supply Chain Risks and Challenges

As supply chains grow more complex, interconnected, and interdependent, exposure to risk also increases, as both the likelihood and knock-on impact of any disruption become harder to predict and identify. For the benefit of this report, we refer to broader definition of supply chains as a network of individual and entities involved in creating and deliver a product which can be connected to IT. Supply chain risks refer to the threats and vulnerabilities associated with products throughout the entire supply chain lifecycle.[8] To manage supply chain risks, there is a need to understand the different threats and vulnerabilities in these complex systems. Further, with more and more supply chains involving IT systems, risks from supply chain cyberattacks are on the rise.

As detailed in the Cybersecurity Supply Chain Risk Management (C-SCRM)[9] program from the National Institute of Standards and Technology (NIST), supply chain threats can be categorized as Adversarial (e.g., tampering, counterfeits, unauthorized production, theft, cyberattacks) or Non-Adversarial (e.g., natural disasters, global pandemics, geopolitical tensions, market changes), where vulnerabilities can be internal (e.g., organizational procedures, insider threats, poor manufacturing and development practices) and external (e.g., supplier bankruptcy).

Further, supply chain risks can be categorized in strategic, tactical, and operational terms (STO Framework).[10]

- At a fundamental level, operational risks describe the day-to-day procedures and processes unfolding on the ground. Mitigating such risks requires comprehensive, real-time

Strategic Risk	› Long-term › External factors › Mega trends › Business model
Tactical Risk	› Medium-term › Transactional › Projects › Financial Risk
Operational Risk	› Day-to-day › Resilience › People, Systems, Processes › Compliance

Figure 1: : STO Framework Risk Categorization

visibility across supply chains to effectively identify and address hazards.

- Tactical risks refer to medium-term risks that pose immediate challenges arising from specific transactional processes and vulnerabilities. These could include risks related to a particular project. As the risk horizon expands from day-to-day operational risks to wider, medium-term risks, there is a possibility of contagion where the risk spreads. Therefore, tactical risks demand that entities (i.e. businesses and organizations) take a step back and perform a broader risk analysis, potentially through scenario planning or modeling approaches like digital twins. Some examples of tactical risks are regulatory changes, currency fluctuations, and labor shortages. However, these are not inherent to the definition of tactical risks, but rather potential outcomes or responses. The key factors are the medium-term horizon and project-specific nature of tactical risks, which require a wider perspective to mitigate compared to short-term operational risks.

- Beyond that, strategic risks are longer-term threats caused by external factors such as changes in the economy, technology, and political instability. Since strategic risks stem from mega trends, entities may need to re-think their models and operations. This overhaul demands a broad, long-term approach including measures such as network-level modeling and simulation, strategic buffer inclusion and sizing, developing longer-term multi-sourcing options, and, in addition to technical measures, may require holistic approaches such as incident response strategies.

Another unintended consequence of increasing complexity is that entities are finding it more difficult to establish visibility across their supply chains. Today, even relatively simple supply chains are built across a range of third-party relationships that include IT services, facilities and operational vendors, cloud service providers, and more. As more entities are introduced into the supply chain, it becomes harder to track the myriad variables that can multiply or over-concentrate risks. Furthermore, supply chains can evolve quickly and, with that, the challenges in managing security and resilience increase.

It is a highly complex and challenging exercise to ascertain the cyber posture of entities involved in various parts of the supply chain. There are no clear widely accepted standards to undertake such assessments, but instead there is a wide variety of country and industry-specific requirements that have arisen over time in different jurisdictions that have added to the compliance and cost burden.

On a positive note, technological innovation and advances are creating new ways for entities to better understand, monitor, and evaluate complex supply chains, providing new capabilities to identify and mitigate risks, respond to incidents, and even anticipate disruptions. Fully harnessing these technologies will require a whole-of-ecosystem approach where stakeholders safeguard and manage risks at the operational, tactical, and strategic levels. Members of the ecosystem include:

1. Key domestic entities (such as CI owners)
2. Third-party vendors and suppliers
3. National- or sectoral-level leaders and regulators
4. International community including international standards bodies and associations

2.3 Country Analysis: Approaches to Enhancing Supply Chain Resilience

Faced with the evolving threat landscape and increasing complexity of supply chains, policymakers in APAC are establishing working groups and developing frameworks and measures to better understand these risks and how to mitigate them. This section looks at the approaches adopted by countries that have been developing measures to enhance supply chain resilience, namely, Japan, South Korea, Singapore, Australia, and New Zealand. The section also covers relevant efforts emerging from international forums like the Indo-Pacific Economic Framework for Prosperity (IPEF) and the G7.

2.3.1 Japan

Economic security and the protection of critical supply chains has been a top concern for Japanese policymakers even before the crisis in Ukraine and its impact on global energy markets. In the context of intensifying US-China strategic competition and China's position as Japan's largest trading partner, Japan passed a far-reaching Economic Security Promotion Act in May 2022[11] that seeks to protect critical technologies and reinforce critical supply chains, while also strengthening cybersecurity among firms working in sensitive sectors or in critical infrastructure in Japan.

The Act's provisions are being implemented on a staggered basis, with some measures not scheduled to be introduced until mid-2024. The Act seeks to mitigate supply chain risks related to materials and products deemed sensitive and does not specifically differentiate between cyber and non-cyber products. However, as part of the Act's implementation, Japan has begun identifying "critical specified technologies" with the goal of promoting and safeguarding capabilities in sensitive technology fields, such as artificial intelligence (AI), quantum, and marine technologies.

In addition to its Basic Policy on Economic Security Promotion[12], the government has published its Basic Guidelines for Securing Stable Supply[13] and its Basic Guidelines for Specified Critical Infrastructure Services to support the Act[14].

These documents outline the key conceptual parameters for the identification and assessment of critical goods and supply chains. This includes assessing the essentiality of specific items and networks for the survival of the Japanese people, examining the potential scope of impact from supply chain disruptions on people's lives and Japan's economic activity, analyzing the difficulty of finding replacements or substitutes, evaluating the dependence or concentration of the supply chains on specific countries or regions, gauging vulnerability to short term disruptions, and others. The policy does not provide specific thresholds for each parameter, but instead allows the government to designate specific critical materials and products.

Under the Act's supply chain provisions, Japanese companies operating in designated sectors are encouraged to prepare plans for promoting the security of supply covering mitigation measures such as diversification of sources, stockpiling measures, improvement of production facilities, options for alternative materials, and others. Once these plans are approved by the Minister with jurisdiction over the industry in question, the government can also provide subsidies, funding, and credit insurance to support their implementation. In addition to these domestic measures, Japan is also engaged in international efforts to promote supply chain security and resilience, including through the G7, the Quad, the IPEF, and a US-Japan-South Korea supply chain early warning system (EWS) pilot announced in August 2023.

Specific to cybersecurity, the Cybersecurity Taskforce under the Ministry of Internal Affairs and Communications (MIC) released their draft ICT Cyber Security Comprehensive Measures 2023[15], which includes new initiatives specific to supply chain cybersecurity risk countermeasures. The draft document proposes that Japan develop 5G security guidelines, Software Bill of Materials (SBOM) requirements, and study the feasibility of analyzing the behavior of smartphone applications. The draft document also emphasizes the importance of building up the cybersecurity capabilities of countries in the Indo-pacific region to address weak-links and vulnerabilities in global and regional supply chains, highlighting Japan's efforts in this area such as the ASEAN-Japan Cybersecurity Capacity Building Center that has been established in Bangkok, Thailand.

2.3.2 South Korea

Policymakers in South Korea are also increasingly concerned about the underlying supply chain vulnerabilities that events such as the pandemic and rising US-China tensions have brought to light.

Like Japan, South Korea has adopted a broad approach by looking at both cyber and non-cyber supply chain risks. The draft Basic Act on Supply Chain Stabilization Support for Economic Security (Basic Supply Chain Act)[16] was introduced in the National Assembly in October 2022. At its core, the draft Act will establish a government-wide management and response system with a new Supply Chain Stabilization Committee as its "control tower".

More specific proposed initiatives include the establishment of an Early Warning System (EWS) for supply chain risks where monitoring is driven by the relevant government ministry, a supply chain stabilization fund to support emergency mitigation measures, and taxation-related funding support for small-and medium-sized industry players to support their supply chain risk management efforts. Notably, the draft law also proposes different tiers of coverage for products and services, including, at its lowest tier, "crisis items" with significant annual import value, "EWS items" that have around 50% dependency on a specific country, and, at the highest-level, economic security items that require pan-government management. The draft Act is still being discussed.

Meanwhile, the Ministry of Science and ICT (MSIT) and the Korea Internet and Security Agency (KISA) have also introduced their own initiatives that focus on cyber supply chain risks. Both MSIT and KISA jointly launched the Zero Trust / Supply Chain Security Forum in October 2022 to discuss how to introduce the Zero Trust principles in South Korea to enhance supply chain security.[17] In July 2023, both agencies jointly launched the Zero Trust Guidelines 1.0[18] that not only emphasizes the importance of adopting a Zero Trust approach to mitigate and minimize cyber supply chain risks, but also provides information on the principles, models, and approaches of Zero Trust Architecture and highlights implementation use cases and challenges to aid real-world deployment.

MSIT has continued to strengthen its response to cybersecurity incidents, including issuing revised guidelines to prevent and respond to ransomware damage[19] to domestic users and companies. KISA also participated in an international joint simulation training with the Asia-Pacific Computer Emergency Response Team (APCERT) to exercise the accident response procedures and responsiveness to supply chain attacks that can lead to large-scale damage.[20]

The Korea Healthcare Computer Emergency Response Team (Korea Healthcare CERT) under the Public Health Sector Coordination Council has also released a Healthcare Cybersecurity Supply Chain Risk Management Guide[21] which advises the healthcare sector on how to develop a supply chain risk management plan, how to incorporate security considerations in selecting vendors, and how to respond to incidents and supplier non-compliance.

2.3.3 Singapore

In response to growing concern about supply chain cyber risks, the Cybersecurity Agency of Singapore (CSA) launched its Critical Information Infrastructure Supply Chain Program Paper in July 2022.[22] The program builds on Singapore's existing CII regulatory regime by introducing five "foundational" initiatives. The first is a toolkit that is meant to help CII owners identify and assess supply chain risks. Specifically, it guides CII owners to inventory their vendors to increase visibility of the cyber supply chain and thereby assess upstream exposure to cyber risks.

The next two initiatives aim to manage and regulate vendors to improve their cybersecurity practices. This is through a handbook of sound contractual terms for cybersecurity requirements for vendors and a certification program to ensure that CII vendors meet baseline cyber supply chain standards. The last two initiatives serve to enhance education and international capacity building and include a learning hub to support knowledge sharing and training of CII stakeholders and a platform for international cooperation.

As the toolkit, handbook, and other initiatives have not been fully rolled out, the implementation details on how Singapore plans to mitigate CII supply chain cyber risks are not publicly available yet.

2.3.4 Australia

Australia's Office of Supply Chain Resilience under the Department of Industry, Science and Resources was established in 2021 to coordinate whole-of-government advice on general supply chain vulnerabilities. The office follows a framework that helps government agencies assess their supply chain resilience and provides policy responses to address the risks. Australian critical infrastructure across 11 sectors is regulated under the Security of Critical Infrastructure (SOCI) Act 2018[23], and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022[24]. This places various obligations on entities, including rules to manage risks across cyber and IT, personnel, supply chain and physical/natural hazards. Additionally, the government can request information,

give directions, or intervene in the case of cyber security incidents impacting the critical infrastructure asset.

Australia also has a range of cyber supply chain risk management frameworks and guidelines that are managed by the Australian Cyber Security Centre (ACSC). A key document is the Critical Technology Supply Chain Principles[25] that provides 10 principles grouped under three pillars: Security-by-Design, Transparency, and Autonomy and Integrity. The principles provide considerations for risk-based identification and assessment of critical technology supply chains, benchmarked with existing internationally-recognized standards.

The ACSC provides more detailed guidelines on the abovementioned considerations through its Cybersecurity Supply Chain Risk Management publication.[26] It includes additional guidelines on the identification of supply chain risks through

its Identifying Cyber Supply Chain Risks[27] publication that details guiding questions on how to identify and assess cybersecurity risks. It also includes a cybersecurity framework known as the Information Security Manual[28], applicable to government entities, that provides cybersecurity principles and guidelines for procurement and outsourcing activities based on internationally-recognized standards.

Additionally, a joint guide by the US Cybersecurity and Infrastructure Security Agency, National Security Agency, the Federal Bureau of Investigation, the UK National Cyber Security Centre, the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, and New Zealand NCSC was released in 19 April 2023 to provide a set of recommendations to help communities strengthen their cybersecurity posture through secure planning and design, protective supply chain risk management, and operational resilience. Known as the Cybersecurity Best Practices for Smart Cities,[29] the document seeks to advance international collaboration and conversation on key priority areas[30] to ensure that smart city infrastructure systems and supply chains are secure, safe, and resilient.

On top of recommendations such as implementing zero trust architecture, enforcing multifactor authentication, applying the principle of least privilege, developing incident responses, and conducting workforce training, the document also provides guiding resources from the various authoring agencies regarding software and hardware supply chains. A similar jointly-developed guiding resource developed by several governments including Australia, Canada, the UK, Germany, the Netherlands, and New Zealand is the Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default document which provides technical recommendations and core principles to software manufacturers in building software security into their design processes.[31]

2.3.5 New Zealand

In 2021, the Government Communications Security Bureau's National Cybersecurity Centre (NCSC) developed the Supply Chain Cyber Security: In Safe Hands[32] resource to help both government and non-government organizations understand and manage their supply chain cyber risks. The document lists three key phases in dealing with supply chain cyber risks: *Identifying, Assessing, and Managing*. The document includes recommendations and resources such as the Protective Security Requirements[33] that include 12 principles of supply chain security to help both public and private sector entities assess their supply chain security; a reference of international and government standards to help entities identify, monitor, and mitigate risks using a policy-based approach including an ISO 31000 risk management framework and the New Zealand Information Security Manual; and the establishment of supply chain risk management programs such as industry-wide information-sharing events and specialist training.[34]

New Zealand has also partnered with countries on joint cyber and supply chain resilience initiatives such as the abovementioned Cybersecurity Best Practices for Smart Cities[35] that seeks to push international collaboration through shared insights and approaches and the Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default[36] document that provides the technical recommendations to design resilient software.

2.3.6 Indo-Pacific Economic Framework for Prosperity (IPEF)

The negotiating parties of IPEF currently represent about 40% of the global GDP with members from Australia, Brunei, Fiji, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Thailand, the United States and Vietnam. At a ministerial-level meeting on the margins of the APEC forum in the United States in May 2023, IPEF countries released a statement regarding a new IPEF Supply Chain Agreement.[37]

The text of the agreement was released in September 2023 and includes 27 articles to build stronger IPEF supply chains. Proposals include aligning on guidance and policies related to trade facilitation; sharing information on best practices through mutual recognition arrangements; developing digital standards and frameworks to support IT interoperability and data flows; fostering increased availability of investments;

publishing laws and regulations related to IPEF supply chains; identify critical sectors or goods; monitoring and addressing supply chain vulnerability; among others.[38]

As part of the IPEF agreement, three new IPEF Supply Chain bodies are proposed to be established to facilitate the cooperation between partner countries including an IPEF Supply Chain Council consisting of senior government officials from IPEF partners to develop critical sector-specific action plans, an IPEF Supply Chain Crisis Response Network as an emergency communications channel, and an IPEF Labor Rights Advisory Board consisting of government, workers, and employers to support the promotion of labor rights in supply chains. The CCAPAC is monitoring the IPEF as a possible platform for greater alignment and harmonization of security requirements across the partner countries.

2.3.7 G7

At the 2023 G7 Summit, a key topic was the diversification of supply chains to ensure resilience during crisis times. Consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, the G7 plans to launch a partnership scheme known as Resilient and Inclusive Supply-chain Enhancement (RISE) by the end of 2023. The scheme aims to support low- and middle-income countries to play a bigger role in midstream/downstream clean energy supply chains.

Specific to cybersecurity, the group updated the G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector in 2022[39] to help entities address their cyber risks and tailor the elements to inform regulatory efforts. The seven elements include governance, risk management process, incident response, contingency planning and exit strategies, monitoring for systemic risks, cross-sector coordination, and third parties in the financial sector. As part of its risk management element, the document advises adopting a risk-based approach to the management of cyber risks through proper identification of third parties and their criticality, conducting cyber risk assessments, ensuring that contracting terms are robust, and providing ongoing monitoring to review the materiality of the risks.

2.4 Commonalities in APAC Regulatory Approaches to Enhancing Supply Chain Resilience

Supply Chain Risk Management and Cybersecurity Supply Chain Risk Management are still relatively new areas for policymakers and regulators in APAC, resulting in some variation in policy approaches as seen in the country outlined above. Despite these differences in approaches, there are also key common strands that we see across countries. These common elements convey the challenges faced and how policymakers are working to address them. In this section, we cover four broad elements that are common across the various countries:

1. Prioritizing Critical Infrastructure (CI) and Building on Existing CI Regulatory Regimes;
2. Establishing Guidelines for Identifying, Assessing, and Managing Supply Chain Risks;
3. Facilitating Education, Training, and Information-sharing;
4. Supporting International Collaboration and Capacity Building.

2.4.1 Prioritizing CI and Building on Existing CI Regimes

Given the ubiquity, broad scope, and complex interdependencies of supply chains and supply chain risks, one of the first and most important challenges that policymakers face in enhancing supply chain resilience is the need to focus and prioritize. In today's world, almost all products and services are a part of a larger supply chain, and these supply chains vary in size, scope, complexity, flexibility, and importance. Trying to develop a one-size-fits-all approach to managing supply chain risks is ineffective and unfeasible.

Policymakers in countries like Australia, Singapore, and even Japan (to some extent)

have opted to start by focusing on areas they had previously already identified as most critical to the wellbeing and security of the country's economy and society. By focusing on CI, these countries narrow the scope of the problem to something more specific and manageable and avoid being paralyzed by the complexity of supply chain risks. It also provides an existing regulatory framework to build on and a limited and familiar set of stakeholders with whom to engage, consult, and co-create regulations. Lessons learnt from these initial efforts to improve the resilience of CI-related supply chains help inform future efforts to manage other types of supply chain risks. Lastly, in an environment where political leadership and public stakeholders are intensifying calls for stronger safeguards, it allows regulators to demonstrate progress without rushing to regulate issues and areas without proper study and assessment.

2.4.2 Establishing Guidelines for Identifying, Assessing, and Managing Supply Chain Risks

Based on the reference approaches in the APAC regions, it is evident that policymakers and regulators recognize the importance of not prematurely rushing into prescriptive and legally binding regulations. Instead, faced with complexity and uncertainty when it comes to managing supply chain risks, regulators have opted to develop guidance materials to explain key principles, desired regulatory outcomes, and outline an iterative, risk-based framework through which government and industry can jointly address problems. Regulators have also actively worked to adopt or align with international best practices in developing their guidance material or jointly develop best practice principles with like-minded countries.

For example, Australia's Cybersecurity Supply Chain Risk Management publication includes additional guidelines on the identification of various cyber supply chain risks such as foreign interference; poor security practices; lack of transparency; indiscriminate access and privileges; and weak business practices.[40] As part of their risk management guidance, the government also provides an Information Security Manual that incorporates cybersecurity principles and guidelines from other supply chain risk management frameworks, including materials from the Canadian Centre for Cyber Security, New Zealand's National Cyber Security Centre, the United Kingdom's National Cyber Security Centre, and the NIST Special Publication 800-161 Rev. 1 on Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.[41] Similarly, ACSC also jointly developed the Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default resource document that acts as a best practice guide authored by cybersecurity agencies across the world.[42]

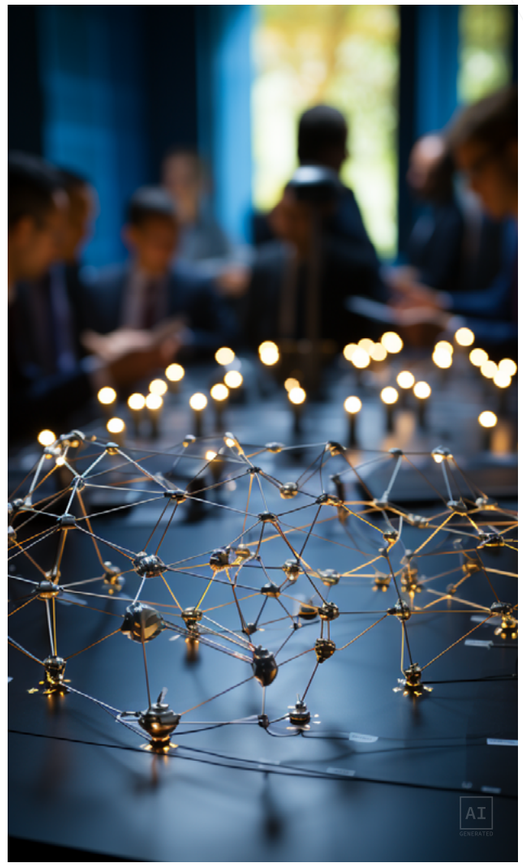
Although there is clear alignment in the preference for a less prescriptive approach that focuses on guidance, one notable area of divergence is the scope and focus of the guidance materials across countries. The guidance developed in Singapore, Australia and New Zealand are pegged at the entity-level and focuses on improving the way domestic entities manage suppliers and supply chain risk. These materials broadly cover key principles for entities to follow when performing supply chain risk identification and impact assessment, including initiatives such as vendor inventories, standard vendor contracts, and, in Singapore's case, vendor certification.

In contrast, while Japan and South Korea do have similar types of materials (e.g., South Korea's Zero Trust guidelines, Japan's Basic Guidelines for Securing Stable Supply), both countries have adopted a broader approach where sector leads and regulators play a role in driving country-level coordination and intelligence and even sector-level funding and financing support. At this early stage, some may question certain national-level initiatives, such as the definitions or thresholds that Japan or South Korea are using to define critical supply chains and goods. Nonetheless, the key point is that some policymakers recognize that individual entities may not have the appropriate threat intelligence or cybersecurity tools to mitigate strategic risks at the national- or sector-level, and that the government sector lead or regulator has a critical role to play.

2.4.3 Facilitating Education and Training

The approaches being adopted by policymakers in APAC include many initiatives to facilitate education, training and information sharing about SCRM and C-SCRM. Policymakers recognize that entities and their employees need to enhance their capabilities in this space to manage the more complex and dynamic landscape of supply chain risks. Businesses and organizations need to invest in their staff and upskill them regularly to ensure that they can capitalize on new technological solutions, adapt to new and evolving threats, and implement operational risk mitigation measures such as the isolation of compromised systems.

For example, a joint guide released by the cybersecurity agencies of Australia and New Zealand details the importance of conducting workforce training and developing incident response and recovery plans that include roles and responsibilities for relevant stakeholders.[43] The guide also provides links to pertinent resources such as the US' Cybersecurity and Infrastructure Security Agency's ICS Learning Portal that includes web-based training and instructor-led training.[44] Another key example is how the Singapore CSA CII Supply Chain Program includes a Cyber Supply Chain Learning Hub that will act as an information exchange platform for the country's cybersecurity agency, sector leads, and critical infrastructure operators to share cyber supply chain threats, implications, and action plans, and provide awareness on the available training resources to help the relevant stakeholders manage their supply chains and bridge the gap in specialist skills and knowledge.[45]



2.4.4 Encouraging International Collaboration and Capacity Building

APAC policymakers have also recognized the fact that the challenges of supply chain risk management extend beyond national boundaries. Supply chains, even relatively simple ones, extend across countries and regions and are only as strong as their weakest link. Beyond the issue of vulnerable products, it is also essential to consider and ensure the resiliency and diversity of sources of supply and facilitate the deployment of strategic technology among like-minded or similarly situated nations. This means that a single entity and even a single country regulator will face natural limits in their ability to mitigate risks across the entirety of the supply chain. In fact, a regional or global view is necessary when it comes to identifying and mitigating strategic level risks, and a systematic approach to assess the security and reliability of products needed in critical deployments. This has incentivized some policymakers to invest in regional-level capacity building.

To this end, policymakers have also been utilizing multilateral platforms to encourage international collaboration, knowledge-sharing, and capability building in C-SCRM. One key example is how IPEF, driven by the US and representing about 40% of the global GDP of the APAC region, has released a statement on an IPEF Supply Chain Agreement that could potentially lead to the development of an IPEF Supply Chain Crisis Response Network. Another important development in this area is at the G7, where members agreed to launch the Resilient and Inclusive Supply-chain Enhancement (RISE) partnership by the end of 2023 that specifically aims to target "low- and middle-income countries".

2.5 Key Takeaways

Supply chain risk management and cybersecurity supply chain risk management are growing priorities among governments in the APAC region. In studying the policy approaches and key initiatives of some of the early movers, a few key commonalities emerge:

1

Focus and Build on Existing CI Regimes

There is a need to manage scope and priority by aligning with critical areas and supply chains. One example is how some countries have opted to focus on CI and build on existing CI regimes.

2

Principles-Based Approach

Policymakers have recognized the need to avoid prescriptive and premature, legally binding regulations and have instead focused on developing guidance materials and an iterative framework in collaboration with the private sector.

3

Education and Training are Key Priorities

New skills are needed to deal with the challenges presented by cyber supply chain risk management that include developing operational know-how and preparing staff to utilize new technological innovations that deal with the added complexity.

4

Risk-Based Approach

Policymakers recognize that the challenges extend beyond national boundaries and that supply chains are only as strong as their weakest link.

In addition to the above, one area of mild divergence is worth note. While many of the initiatives from the various countries covered focus on guidance and safeguards to be implemented at the organization-level (e.g., vendor inventory, supplier management), Japan and South Korea have adopted approaches that acknowledge the role of the government or sector-lead in implementing measures to support risk mitigation at the national-, sectoral-, and strategic level, where individual companies would not have the appropriate threat intelligence or tools.

Chapter 3
Measures and Mechanisms to Enhance Supply Chain Resilience

3.1 Introduction

Enhancing the resilience of the cyber supply chain ecosystem is critical to safeguarding national and regional socio-economic stability. In addition to being able to mitigate threats and respond to incidents, it is important to build a trusted environment to fully realize the benefits of trade and digital technologies. However, dealing with the wide scope and intricate complexities of cyber supply chain risks brings its own new set of challenges that need new solutions.

This section builds on the APAC policy approaches discussed above and takes the unique challenges of C-SCRM into consideration to outline key measures that can be undertaken to enhance Cybersecurity Supply Chain resilience. To provide a framework for us to approach this multi-faceted issue, we will engage the topic on four different levels of hierarchy:

1 **Infrastructure-level:** At the most fundamental level, each cyber product or service constitutes a range of foundational elements that can be part of different supply chains.

2 **Entity-level:** Each entity has its own set of vendors or suppliers, requiring an assessment of each supplier and its upstream dependencies to understand and address potential sources of risk.

3 **National- and Sector-level:** Strategic level risks can impact supply chains at the network level (i.e., network of suppliers within a jurisdiction) and may require mitigation measures on a national or sector-wide scale.

4 **Global- and Regional-level:** Supply chains are built across different trusted countries and regions with redundancy and resiliency so as not to fall prey to a single point of failure.

3.2 Infrastructure-level

3.2.1 Device and Hardware

Sophisticated cyberattacks increasingly seek to compromise the network infrastructure by attacking network devices like routers, switches, wireless access points, and user endpoints at a hardware-level. By doing so, attackers can eavesdrop on sensitive communications, steal or manipulate data, and launch attacks against other parts of the network. This includes advanced persistent threats that modify the underlying hardware or device software.

These threats can go undetected for months, or even years, inflicting devastating damage. Cisco's Talos threat intelligence organization has documented numerous attacks against network devices and, along with the US and UK government[46], has warned about state-sponsored campaigns against global network infrastructure[47].

Trusted Platform Modules (TPMs)[48] are one solution on a device and hardware infrastructure level. TPMs are specialized, tamper-resistant chips that verify device authenticity and integrity to protect against counterfeiting and malicious

hardware/software attacks. TPMs make it possible to do validation of device configuration, secure patching, use digitally signed images, secure boot, and other technologies to establish trust in devices and operating systems. TPMs also provide robust security services like random number generation, secure key management, and can enhance disk encryption and device authentication features. As such, TPMs are a key capability for strengthening hardware device security and building infrastructure resilience at a foundational level.

Though some manufacturers implement TPM capabilities in hardware devices, the features may not be enabled in software or fully integrated with system level checks and onboarding processes to detect compromised infrastructure. It is important that countries recognize the risks posed by compromised infrastructure hardware and guide suppliers to adopt and fully implement products that leverage TPM key capabilities.

3.2.2 Software

3.2.2.1 Secure Software Development Framework (SSDF)

NIST published the Secure Software Development Framework (SSDF) Version 1.1 in February 2022 as a set of "fundamental, sound, and secure software development practices" to help software producers reduce the number of vulnerabilities in released software and reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities.[49] SSDF was devised in response to the Cybersecurity Executive Order in the US as a best practice guide to managing software risks.

Because its security practices map well to the existing risk management of software development life cycle (SDLC), part of SSDF is being adopted by software providers to the US government in 2023. In light of the Office of Management of Budget (OMB) memorandum on "Enhancing the Security of Software Supply Chain through Secure Software Development Practices" (M-22-18), it is expected that US government agencies will require their software vendors to provide assurance that the software they provide to these agencies is securely developed.[50]

The SSDF does not create new requirements but leverages existing standards and best practices to help entities document their secure software development practices. Entities can integrate the SSDF throughout their practices, express secure software development processes to third-party suppliers, and evaluate software that meets the practices described in the SSDF. Importantly, the SSDF does not prescribe how to implement each practice.

3.2.2.2 Software Bill Of Materials (SBOM)

According to the Cybersecurity and Infrastructure Security Agency (CISA), a SBOM is a "nested inventory" or a "list of ingredients that make up software components"[51] and provide a standardized approach to understanding what is in an application. In 2021, the US Biden Administration issued an Executive Order (EO) to improve the country's cybersecurity by permitting federal agencies to ask federal contractors to provide government customers with a SBOM for their products.[52]

3.2.3 Cloud Services

Cloud services have become widely adopted across public and private sector organizations, providing convenient on-demand access to computing resources, applications, and data storage. Understanding how cloud services fit into enterprise cyber supply chain security management is not necessarily complex. Key internationally-recognized standards tailored to the cloud environment can enable organizations to evaluate and certify the security posture of providers across the full supply chain, providing assurance and transparency between customers and providers of cloud services.

The ISO 27000 series of standards include several controls relevant to cloud security:

- ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO/IEC 27002 best practice guidance. It includes the development and implementation of an Information Security Management System (ISMS) which defines how cloud service providers manages security in a holistic, comprehensive manner.
- ISO 27017 focuses specifically on information security controls for cloud services based on ISO 27002, while ISO 27018 covers protection of personally identifiable information (PII) in the cloud.
- ISO 27036 provides guidance on the information security risks associated with cloud computing and how to mitigate them through a structured approach to risk assessment, treatment, and ongoing monitoring.

The Cloud Security Alliance has also published various frameworks to help organizations assess and certify the security posture of cloud providers. The Consensus Assessments Initiative Questionnaire (CAIQ) provides a standard set of security controls that cloud customers can use to evaluate providers. The Alliance's Security, Trust and Assurance Registry (STAR) offers a free publicly-accessible registry where providers can publish compliance reports against key industry standards.

To gain confidence in the integrity of the cloud supply chain, organizations should examine providers' conformance to internationally-recognized standards and best practices for supply chain risk management. Although cloud providers handle much of the underlying security, customers remain responsible for securing data, applications, operating systems, and identities in the cloud. With proper due diligence and implementation of standards-based controls and best practices, organizations can enhance visibility and mitigate risks in cyber supply chain for cloud services.

3.3 Entity-level

3.3.1 Adopting a Technology Neutral and Outcome-focused Approach

Business impact due to unmitigated supply chain risk is the new norm. To meet the new challenges of today's increasingly complex global economic environment, entities must capitalize on emerging technologies and innovative solutions that can monitor evolving supply chain networks, support incident response measures, and even predict threats. By utilizing cloud services together with new technologies such as AI, blockchain, predictive analytics, and digital twins, industry leaders have been developing new solutions that have the potential to not only limit the damage of supply chain breaches, but to enable businesses and organizations to improve their operational efficiency and sustainability.

Regulators should adopt a technology-neutral and outcome-focused approach to give industry sufficient regulatory space and flexibility to seek out innovation and implement solutions that can keep pace with the threat landscape. Instead of trying to put in place hard regulations, it is more effective at this stage to provide guidance on key relevant security concepts such as Zero Trust architecture (like South Korea has done), vendor/supply chain business continuity planning, and others.

In addition, it is also important to ensure that the underlying technologies themselves do not end up being over-regulated. For example, both Japan and Australia have designated AI as specified critical technologies under their respective regimes. This is certainly understandable given the socio-economic significance of AI. However, if either country over-regulated AI development and deployment because of its status as a critical technology, that would severely limit the industry's ability to utilize it to solve supply chain challenges, as well as stifle innovation in AI generally. Instead, governments should consider technology neutral approaches. Constraints can be placed on unacceptably high-risk use cases, but the general rule should be closely linked to the risk of harm and the consequences in terms of damage should an adverse outcome occur, rather than be targeted at specific technologies.

3.3.2 Supporting RegTech and Regulatory Innovation

On top of ensuring that industry has the space to adopt new solutions, policymakers should also consider going one step further to actively promote and support the development of Regulatory Tech (RegTech) and other innovations that can enhance supply chain resilience.

RegTech is the use of technology to enhance risk management and regulatory compliance, especially in financial institutions.[53] RegTech helps to manage regulation monitoring, compliance, and reporting by keeping track of new regulations as they emerge. As such, innovative technology such as RegTech helps to reduce time and cost required for compliance, freeing up resources. An example of RegTech is blockchains that can be used to create tamper-proof logs of transactions in a supply chain, helping to ensure transparency and compliance with regulations related to traceability and product origination.

Policymakers and sector leads should consider establishing regulatory sandboxes to allow solution providers to collaborate, experiment and co-create new RegTech solutions to secure supply chains while enhancing compliance. In this way, governments can help to accelerate innovation and protect domestic operators while building up their own SCRM capabilities and knowledge through the facilitation of pilots and trials.

The first step would be to work together with industry to develop joint problem statements that address regulatory concerns and industry challenges. These could range from developing a solution to detect patterns that reveal supply chain problems as they occur, to developing a means to automate responses and mitigate supply chain disruptions.

3.4 National- and Sector-level

3.4.1 Sector-level Intelligence and Risk analysis

Business operators must be able to manage their supply chain risk, but there are natural limits to what an individual business operator can accomplish by themselves. Supply chain challenges cut across singular entities, industries, countries and even regions. As individual business operators, their access to intelligence and information on wider threats and supply chain movements is limited. Further, their ability to respond to and mitigate larger sector-wide or nation-wide disruptions is also limited.

Regulators or sector leads are better placed to take on the role of the control tower – to develop sector-level intelligence and risk analysis, and to oversee the larger, strategic picture and coordinate across the industries. This will facilitate a whole-of-ecosystem approach to threat identification and emergency response beyond the capabilities of individual operators.

3.4.2 Co-creating Innovative Solutions

Supply chains may have increased in complexity and diversity in recent years, but they are not a new phenomenon. Industry leaders have been developing solutions and providing services to help entities manage their supply chains for decades. As such, they not only have decades of experience solving supply chain risk management problems, but also decades of valuable data on supply chains.

- For example, the Amazon Web Services (AWS) Supply Chain application is used to help businesses and organizations increase supply chain visibility and analyze data across multiple supply chains to generate forecasts.[54]
- Cisco's Secure Network Analytics, which was used to defend against the SolarWinds supply chain attack, helps detect software supply-chain attacks in real-time to identify and isolate threats.[55]
- The Qualcomm Aware platform helps operators address supply chain ecosystem fragmentation and harness real-time data to support supply chain digital transformation.[56]
- Beyond direct solution providers, policymakers can also consider consulting industry leaders like Becton Dickinson who have been managing critical medical supply chains and delivery of care supply chains for decades.

Developing the capability to monitor and mitigate strategic supply chain risks at the national-level will be a challenging task, which is

why policymakers should tap industry expertise and seek out opportunities for public-private partnerships to collaborate on new solutions tailored to address sector-level risks. Examples could include modeling and simulation capabilities for networks of supply chains, such as a digital twin, or real-time analytical systems to forecast strategic buffer inclusion and sizing.

3.4.3 Supporting and Empowering Industry

Policymakers should also consider providing additional support to entities to assist them in enhancing their supply chain resilience and risk management. For example, providing subsidies or funding support to small and medium-sized enterprises (SMEs) to enhance their supply chain risk management capabilities would increase overall industry investment to supply chain resilience. Noting the importance of building up employee expertise in this area, policymakers should also consider providing financial or non-financial support for training and education related to supply chain risk management.

3.5 Global- and Regional-level

3.5.1 Harmonization and Global Best Practices

With supply chains growing more complex and involving multiple stakeholders globally, a harmonized set of policies and frameworks is beneficial to foster consistency, efficiency, and collaboration across the set of stakeholders involved in building supply chain resilience. Initiatives from international forums such as the new IPEF Supply Chain Agreement and the G7's Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector are commendable steps towards achieving harmonization across different standards and practices.

However, many of these initiatives are non-binding and high-level in their commitments and approaches due to their global nature. To ensure that supply chains remain resilient, it is critical that harmonized frameworks provide more detail and practical implementation mechanisms. Policymakers in APAC should consider using regional platforms such as ASEAN to drive specific harmonization recommendations in the region through cooperative mechanisms such as working groups.

At a higher level, strategic coordination is needed to ensure that national supply chain strategies address issues of resiliency and redundancy. There is a need to establish mechanisms for countries to retain the ability to readily obtain the necessary source materials, components, and finished goods from a competitive market of trusted suppliers.

3.5.2 Capacity Building

Capacity building is an essential way for countries with more mature and robust resources to support neighboring states in aligning policies and frameworks with international standards through training programs, technical assistance schemes, and technology transfer exercises.

For example, the ASEAN-Japan Cybersecurity Capacity Building Centre aims to address the vulnerabilities in the regional supply chains and highlights Japan's efforts to strengthen the cybersecurity capacity in the region. As supply chains grow increasingly complex and globalized, the resilience of a nation's supply chain will be affected by the security of their regional and global stakeholders, which is why policymakers should consider similar initiatives to build up the long-term resilience of supply chains in the region.

Regulators and policymakers, specifically those with cybersecurity portfolios, should consider building up a platform or way for regional stakeholders to drive synergies on cybersecurity frameworks and supply chain resilience building. For example, the anglosphere's cybersecurity agencies (i.e., Australia, Canada, New Zealand, United Kingdom, and the United States) published a joint guide to advance international collaboration and conversation on key supply chain areas by including resources from the various authoring agencies and providing technical recommendations and core principles agreed across all five countries. Examples for a regional initiative could include establishing information sharing platforms and setting up training workshops to share experiences and knowledge among participating countries.

Chapter 4
Conclusion and a Call to Action – Recommendations on development of CII Supply Chain Security in APAC markets

The increasing interconnectedness and complexity of global supply chains has introduced new vulnerabilities that can have severe consequences for national security and economic stability. Recent disruptions have made it clear that a more proactive and collaborative approach is needed to enhance resilience.

While APAC countries have made strides by focusing on critical infrastructure and developing risk-based frameworks, these efforts have been largely reactive and siloed. True resilience requires a systemic approach across the entire supply chain ecosystem and coordination across the region. CCAPAC is supportive of the development of a strong cybersecurity ecosystem in Asia Pacific and offers the following recommendations for strengthening regional supply chain policy.

Recommendation #1:
Foster Resilience through Public-Private Collaboration

Policymakers should shift mindsets from compliance to resilience. The goal should not be to just identify risks and meet security standards, but to build dynamic systems that can rapidly adapt to disruptions. This demands greater integration between the public and private sectors to coordinate intelligence, funding, and emergency response.

Recommendation #2:
Encourage Innovation and Experimentation

Regulators also need to balance security with innovation. Prescriptive regulations could undermine industry efforts to leverage new technologies to predict and mitigate supply chain disruptions. An outcome-focused approach allows room for the experimentation needed to develop robust RegTech solutions.

Recommendation #3:
Take a Comprehensive Approach to Strengthen Infrastructure Resilience

To enhance cyber supply chain resilience at the infrastructure level, policymakers should promote the adoption of critical hardware security capabilities like TPMs and look for opportunities to embrace still-evolving capabilities like SBOMs without setting mandates prematurely. Regulators should encourage secure software development frameworks and refer to internationally-recognized standards for cloud security in any certification regimes.

Recommendation #4:
Promote Regional Cooperation and Joint Capacity Building

No single nation can address these transborder challenges alone. Regional cooperation mechanisms to align standards and share best practices are critical to avoiding fragmented requirements that increase costs for businesses and organizations. Joint capacity building initiatives also empower neighboring states to uplift cybersecurity, addressing vulnerabilities that could spread across borders.

Ultimately, enhancing cyber supply chain resilience is not just a technical process, but an adaptive mindset. As interdependencies deepen, stakeholders across the ecosystem must cooperate to achieve collective resilience. Policymakers play a key role in fostering this collaboration. By providing the right incentives and environment, they can catalyze a new paradigm for secure and resilient digital trade.

CCAPAC is committed to positively shaping the cybersecurity environment in APAC, and we welcome discussions with governments and cybersecurity agencies to further strengthen and develop a strong and secure ecosystem in APAC. Get in touch and visit our website at https://ccapac.asia for more thought leadership and research, or to arrange for a discussion or capacity building engagements.

Endnotes

1 https://ccapac.asia

2 Supply chain disruptions in US and Europe reached around USD4 trillion in 2020. https://www.cips.org/supply-management/news/2021/march/total-cost-of-supply-chain-disruption-in-2020-was-4tn/

3 https://supplychaindigital.com/top10/timeline-causes-of-the-global-semiconductor-shortage

4 https://www.reuters.com/markets/commodities/companies-respond-chinas-curbs-gallium-germanium-exports-2023-07-06/

5 https://www.reuters.com/business/energy/year-russia-turbocharged-global-energy-crisis-2022-12-13/

6 On average, the cost of cyberattacks on supply chains is USD4.35 million per incident (e.g. the Colonial Pipeline attack in 2021 had a direct impact of USD4.4 million in ransom but resulted in additional indirect financial and socio-economic repercussions). https://www.fortressinfosec.com/blog/cost-of-cyber-attacks-on-supply-chains

7 https://www2.bluevoyant.com TheStateofSupplyChainDefense2022Report

8 https://csrc.nist.gov/glossary/term/supply_chain_risk

9 https://csrc.nist.gov/csrc/media/Projects/cyber-supply-chain-risk-management/documents/C-SCRM_Fact_Sheet.pdf

10 https://goatrisksolutions.com/risk-identification-and-risk-evaluation/

11 https://www.cao.go.jp/keizai_anzen_hosho/

12 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonhoushin.pdf

13 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin1.pdf

14 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf

15 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00169.html

16 https://www.korea.kr/briefing/pressReleaseView.do?newsId=156531084

17 https://www.koit.co.kr/news/articleView.html?idxno=104823

18 https://www.kisa.or.kr/2060205/form?postSeq=20&page=1

19 https://www.kisa.or.kr/402/form?postSeq=2299&lang_type=KO

20 https://www.kisa.or.kr/402/form?postSeq=2304&lang_type=KO

21 https://www.kisa.or.kr/2060205/form?postSeq=20&page=1

22 https://www.csa.gov.sg/Tips-Resource/publications/2022/cii-supply-chain-programme-paper

23 https://www.legislation.gov.au/Details/C2022C00160

24 https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/slacip-bill-2022

25 https://www.homeaffairs.gov.au/cyber-security-subsite/files/critical-technology-supply-chain-principles.pdf

26 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/cyber-supply-chain-risk-management

27 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/identifying-cyber-supply-chain-risks

28 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism

29 https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-smart-cities

30 Recommendations from the Cybersecurity Best Practices for Smart Cities document include having secure planning and design (applying the principle of least privilege, managing changes to internal architecture risks, protecting Internet-facing services), having proactive supply chain risk management (having security requirements and oversight over the software supply chain, assessing risks in the hardware and IoT device supply chain, managing cloud service providers), and ensuring operational resilience (implementing technology to maintain backup systems and data, conducting workforce training, developing incident response and recovery plans).

31 https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf

32 https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

33 https://www.protectivesecurity.govt.nz/governance/supply-chain-security/principles-of-supply-chain-security/

34 https://www.nzism.gcsb.govt.nz/

35 https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-smart-cities

36 https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

37 https://id.usembassy.gov/press-statement-on-the-substantial-conclusion-of-ipef-supply-chain-agreement-negotiations/

38 https://www.commerce.gov/sites/default/files/2023-09/2023-09-07-IPEF-Pillar-II-Final-Text-Public-Release.pdf

39 https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2022-G7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector.en.pdf

40 https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Identifying%20Cyber%20Supply%20Chain%20Risks%20%28May%202023%29.pdf

41 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-procurement-and-outsourcing

42 https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

43 https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf

44 https://www.cisa.gov/ics-training-available-through-cisa

45 https://www.csa.gov.sg/Tips-Resource/publications/2022/cii-supply-chain-programme-paper

46 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108

47 https://blog.talosintelligence.com/state-sponsored-campaigns-target-global-network-infrastructure/

48 ISO/IEC 11889

49 https://csrc.nist.gov/Projects/ssdf

50 https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

51 https://www.cisa.gov/sbom

52 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

53 https://br-ag.eu/2023/01/23/what-is-regtech-and-why-is-it-gaining-traction/

54 https://docs.aws.amazon.com/aws-supply-chain/latest/userguide/what-is-service.html

55 https://blogs.cisco.com/security/detecting-and-responding-to-solarwinds-infrastructure-attack-with-cisco-secure-analytics

56 https://supplychaindigital.com/digital-supply-chain/qualcomm-aware-will-speed-up-supply-chain-transformation

COALITION FOR CYBERSECURITY IN ASIA-PACIFIC

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