(SG

CSA
SINGAPORE

Critical Information Infrastructure Supply Chain Programme

A National Effort In Managing
Cyber Supply Chain Risks

About Cyber Security Agency

Established in 2015, the Cyber Security Agency of Singapore (CSA) seeks to keep Singapore's cyberspace safe and secure to underpin our National Security, power a Digital Economy, and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with Sector Leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cyber security awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

About Boston Consulting Group

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organisations to grow, build sustainable competitive advantage, and drive positive societal impact. Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organisation, fuelled by the goal of helping our clients thrive and enabling them to make the world a better place.

Contact

If you have any feedback on this publication, or wish to find out more about Singapore's efforts in cybersecurity, please visit **www.csa.gov.sg** or contact us at **contact@csa.gov.sg**

Contents

Foreword

The COVID-19 pandemic has accelerated Singapore's digitalisation and increased the complexity of interconnectivity between users, service providers and their vendors. While digitalisation has catalysed the adoption on technology, it has also resulted in a growing reliance on vendors to support the delivery of essential services and organisations' day-to-day operations. As our supply chains increase in complexity, so does our reliance on vendors and sub-vendors, and we do not have adequate visibility of their security posture.

We have to recognise the challenges that digitalisation and ubiquitous connectivity brings – a more interconnected and complex cyber supply chain increases the attack surface and exposes us and our vendors to additional cybersecurity risks. Cyber threat actors can exploit such interdependencies to target organisations by exploiting weak links and trusted relationships in the supply chain. Organisations take on unknown risks of cyberattacks through sub-vendors when they do not have full visibility of their cyber supply chain. Threat actors do not discriminate between industries or organisations: financial institutions, the healthcare industry and power plants have all been targeted by attacks that are capable of disrupting, damaging, and degrading essential services.

There is an increased urgency to focus on cyber supply chain security because threat actors have turned to those attacks instead of targeting organisations directly. Cyberattacks against supply chains are difficult to guard against because the attack compromises part of the trusted IT ecosystem, which in turn can affect a disproportionate number of organisations through a single attack vector. A successful breach in the supply chain, as seen in the SolarWinds incident in 2020, provides cyber threat actors a single pivoting point to multiple victims. The compromise of a trusted supplier – or a popular and widely-used product – can result in massive and widespread repercussions worldwide, as victims could include major vendors with huge customer bases. Cyber threats are transboundary, and the interconnectivity of the Internet allows attacks to be performed speedily, with no geographical limitations. Some organisations were infected with ransomware that spread through their managed service providers, as a result of hackers exploiting a zero-day vulnerability in a popular Kaseya product. Such incidents understandably raised questions

about the prevalence of risks from vendors and the cybersecurity of supply chains. Do these incidents portend a rising trend? Can we trust our hardware and software vendors? Where do our networks end and where are the gateways we need to protect?

The cyber supply chain issue is multi-faceted and multi-layered, and there are seldom any "perfect" or "easy" answers to this wicked problem. The increasing complexity of supply chains affects both public and private sectors and is both a domestic as well as an international challenge. Addressing supply chain risks must be a multi-pronged effort. The cyber supply chain is only as strong as its weakest link. It was with this challenge in mind that CSA conducted consultations with stakeholders, regulators, and industry experts to understand their posture and insights on cyber supply chain risk. With these insights, CSA will drive initiatives to enable the maturity and aid these organisations in their management of cyber supply chain risks.

This CII Supply Chain Programme is our approach to ensure that Singapore remains cyber resilient. We will continue to address core challenges to reach aspirational resilience goals, with CSA, Sector Leads, CIIOs and vendors working together, hand in hand. Through the cooperation of stakeholders, vendors and regulators, the resilience of the Critical Information Infrastructures will be further bolstered against cyber supply chain risks.

David Koh
Commissioner of Cybersecurity and
Chief Executive
Cyber Security Agency of Singapore

Executive Summary

The availability of Critical Information Infrastructures (CIIs) to provide essential services is pivotal to the functioning of Singapore. Organisations have rapidly digitalised their operations to unlock the benefits of technology, but cyber threats have increased in scale and sophistication, placing CIIs at increased risks. A style of cyberattack increasing in prominence is the supply chain attack, where the threat actor compromises a vendor who has a trusted relationship with the customer. The threat actor exploits the supply chain ecosystem by using this trusted connection to bypass the customers' defences to pivot into the customers' environment.

As CIIs consist of complex and multifaceted cyber supply chain networks, the risks lurk in the deeper layers of the cyber supply chain. However, the current approaches to vendor risk management processes are not future-ready to address these evolving challenges for CIIs, as organisations can no longer mitigate systemic cyber supply chain risks individually. The CII Supply Chain Programme is a national programme to enhance the visibility and management of these risks and create structures for stakeholders in the ecosystem to collaborate to improve cyber supply chain resilience.

The Programme outlines five foundational initiatives to begin the journey to address the cyber supply chain challenges facing CIIs at organisational, sectoral, national, and international levels, including the development of a:

1. **Toolkit** for CIIOs to help them identify and inventory vendors, assess and rate their cyber supply chain risks using a standardised vendor management methodology. The goal is to aggregate a national view of all Tier 1 CII vendors and progressively move towards an increased depth of visibility of the cyber supply chain.

2. **Handbook** to provide a repository of sound contractual terms for having cybersecurity requirements in their vendor contracts. The handbook enables CIIOs to improve negotiations with their vendors towards improved cybersecurity practices by helping to place group pressure on vendors to motivate them to achieve an improved cybersecurity posture for their products and services.

3. **Certification programme** for CII vendors to meet a set of baseline cybersecurity requirements for cyber supply chain. Seeking standards and certification incentivises vendors to improve their cybersecurity capability.

4. **Learning hub** to share knowledge, sound practices and training resources of cyber supply chain risk management for CII stakeholders. The learning hub increases the awareness and appreciation of cyber supply chain risks to senior leaders and procurement stakeholders to elevate the topic from technological concern to organisational imperative.

5. **Platform for international cooperation** to initiate close collaborations and working relationships with international government counterparts and industry groups to collectively address cyber supply chain resilience.

The aspiration of the Programme is to foster the various stakeholders in the ecosystem to work together to reduce cyber supply chain risks, create a catalyst for change and elevate the state of cyber resilience of Singapore's essential services.

What does success look like?

Initiative 1: CII Cyber Supply Chain Assessment Toolkit

- Up to date visibility of CII cyber supply chain

- Derivation of insights of cyber supply chain risks and potential concentration risks at national, sectoral and organisational level

- Real time transparency in cyber supply chain risks to the nth level, shortening incident response time

Initiative 2: Cyber Contractual Handbook for CIIs

- Living document of sound cybersecurity contractual terms that incorporates specialist advice and learnings from both public and private CIIOs for continuous improvement

- New "norm" of higher standard cybersecurity contractual requirements - uplifted general standards of vendors with CIIOs using contractual terms of higher standard

- Prioritised critical cyber contractual clauses that require national / sectoral efforts for standardisation and negotiation

Initiative 3: Vendor Certification Programme

- Aligned baseline security hygiene of vendors among CIIOs to national regulations and international standards

- Curated Programme that recognises efforts made by vendors to uplift and achieve cyber security standards and certifications

- Organisations with stronger assurance mechanisms are selected to create positive market incentives towards improved resiliency of the cyber supply chain

Initiative 4: Cyber Supply Chain Learning Hub

- Information exchange platform among CSA, Sector Leads and CIIOs to share cyber supply chain threats, information, implication and action plans based on the specific data points collected and insights aggregated

- Cross-functional knowledge sharing platform and awareness training resources to Sector Leads, CIIOs, business functions that manage CII supply chain and vendors focusing on cyber supply chain risk management

- Bridged skills and expertise gap through knowledge sharing among organisations within the same sector and across different sectors

Initiative 5: International Cooperation

- Increased collective power and negotiation leverage for countries to request for higher baseline cybersecurity hygiene from vendors

- Enhanced efficiency in proactive intervention at the inter-government level to mitigate global supply chain risks instead of leaving it to market forces

- Exchange supply chain risk management methodologies and sound practices with global partners to keep the cybersecurity risk management measures up to date

What is in it for stakeholders?

	Sector Leads	CIIO	Vendors
CII Cyber Supply Chain Assessment Toolkit	Visibility into sectoral CII cyber supply chain to derive insights and potential concentration risks	Visibility and insights of cyber supply chain risks, to improve the cyber resilience of CIIs	Identify cyber supply chain gaps and mitigation measures through the assessment toolkit
Cyber Contractual Handbook for CIIs	Contribute and access to a repository of sound cybersecurity contractual clauses to aid in negotiation and procurement efforts in managing vendor contracts across the vendor lifecycle	Contribute and access to a repository of sound cybersecurity contractual clauses to aid in negotiation and procurement efforts in managing vendor contracts across the vendor lifecycle	Build confidence in provision of services through sound contractual clauses
Vendor Certification Programme	Guide direction of the certification scheme to consider sector-specific requirements and industry-relevant standards and certifications that can promote cyber supply chain resilience of vendors in the sector	Clarity of defined baseline cybersecurity requirements as the minimum standard required of CII vendors and boost confidence levels of CIIOs that vendors have achieved a set of baseline cybersecurity controls	Recognition for vendors who have achieved cybersecurity standards and certification, and boost brand value and business interest through competitive cybersecurity advantage
Cyber Supply Chain Learning Hub	Access to information exchange platform, knowledge sharing platform and awareness training resources	Access to information exchange platform, knowledge sharing platform and awareness training resources	Access to knowledge sharing platform and awareness training resources
International Cooperation	Opportunities to collaborate with international groups and counterparts in other countries of the same sector and industry to facilitate information sharing on sound practices for cyber supply chain	Opportunities to collaborate with international groups and counterparts in other countries of the same sector and industry to facilitate information sharing on sound practices for cyber supply chain	Under this initiative, there will be efforts to align standards for baseline cybersecurity requirements of vendors with international counterparts, driving a consistent global approach to risk management

Chapter 1: Introduction

1.1. Cyber Resilience: A National Concern for the Availability of Essential Services in Singapore

In recent years, the adoption and utilisation of digital technologies are continuing to accelerate, and it has become a pervasive part of our digital way of life. This acceleration is transforming the world in which we live in at a rapid pace, creating a new digitally connected landscape markedly different from that seen even a decade ago.

The COVID-19 pandemic has fundamentally changed how we work and live with the pace of digitalisation accelerating even further. It is triggering a more rapid shift towards digital transformation, catalysing even greater reliance on technology across all businesses and sectors.

During the pandemic, the prevalence of digital platforms and technologies has grown as individuals and organisations turn to digital solutions to maintain everyday operations. Employees have shifted to working from home through remote working technologies, while traditional brick-and-mortar businesses have transitioned their services online. In a recent survey, 73% of organisations in Singapore acknowledged they were accelerating their pace of digitalisation in response to the pandemic[1].

Industry 4.0 powers connectivity

The ongoing Fourth Industrial Revolution (Industry 4.0) underpins a landscape of growing connectivity, with technology trends such as the Internet of Things (IoT) and the use of 5G technologies providing opportunities to digitalise segments and functions within organisations that are previously disconnected from the Internet. Projections expect the number of connected IoT devices to reach 75 billion worldwide by 2025[2] and this places pressure on organisations to quickly find solutions to manage and secure an exponentially increasing web of network connections.

Organisations are increasing their reliance on technology

As governments and businesses digitalise, they become increasingly reliant on connected digital infrastructure and services to achieve their desired outcomes. This transition disrupts existing business practices and creates operational instability that introduces new vulnerabilities and expands the attack surface.

With the growing reliance on technology, the impact of a disruption to the availability of digital infrastructure or services on organisations and individuals is likewise increasing. Organisations are faced with the reality that disruption to digital infrastructure can potentially result in a fundamental disruption to their businesses. The ramifications of digital disruption are only likely to grow more profound as the digital transformation landscape grows over the long term.

The cyber threat continues to grow

As digitalisation increases, cyber threat actors are capitalising on this trend. The volume and sophistication of cyberattacks are increasing as the attack surface expands. Advances in technology are simplifying the execution and decreasing the cost of cyberattacks. In parallel, the requirements for defence are growing in complexity and cost.

Estimates project that global losses from cybercrime will exceed USD6 trillion by the end of 2021, up from USD3 trillion in 2015 and increase to USD10.5 trillion annually by 2025[3]. As the scale of impact from cyber risks increases, so does the breadth of the impact. These now extend beyond simple financial and data losses to significant operational disruption, long-term reputational damage for organisations. They may also impact the delivery of critical services.

Vulnerabilities can be exploited to disrupt Singapore's way of life

As a hyper-connected business hub with a clear direction to leverage the potential of digitalisation and innovation, cyber threat trends are particularly pressing for Singapore. Singaporeans consume essential services powered by digital technologies daily. These include services such as electricity to power homes and connected technologies to share digital time with loved ones.

Underpinning the provision of essential services is the CII. A CII is a computer or computer system 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. Reliable delivery of essential services is pivotal to the efficient functioning of Singapore as a country.

Increasing digitalisation and expansion of connected systems in Singapore is not just limited to commercial organisations and individuals, it has permeated into the backbone of CIIs. Critical Information Infrastructure Owners (CIIOs) (organisations that own and operate CIIs) are keen to take advantage of digitalisation's efficiency and innovation benefits and capture new streams of value to provide superior services to Singapore.

CIIs are now increasingly reliant on internet-connected systems to power their operations, replacing technologies previously disconnected from the Internet. Examples include control systems for monitoring chemical pumps in water networks or switches for distribution in the energy grid. This shift exposes CIIs to a broader range of threats and vulnerabilities and reflects a fundamental challenge at the heart of digitalisation.

Digital technologies provide ways to improve lifestyles, well-being, and the economy, but reliance on this infrastructure makes the country vulnerable to disruptive cyberattacks. These attacks are intensifying in both scale and sophistication and could ultimately lead to a disruption that impacts the lives and livelihoods of Singaporeans.

Critical Information Infrastructures (CIIs) in Singapore
CIIs are digital systems that support the delivery of essential services. Today, CIIs have been identified from 11 critical sectors — Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency Services, and Water. To ensure that cyber threats do not disrupt our essential services, the Government has put in place a three-tier framework to strengthen the cyber resilience of CIIs.

Cyber Security Agency of Singapore
CSA, as the independent national authority on cybersecurity, monitors and regulates the CII sectors. At the same time, CSA actively supports sector leads and CIIOs to improve their situational awareness and build up their capabilities.

Sector Lead
Each CII sector has a sector lead who works closely with CSA. They are the natural regulators of the CIIOs and have a good grasp of the unique operating and business environment — and risks — of their respective sectors. They are best placed to guide the appropriate balance point of cybersecurity, usability, and cost.

CII Owner (CIIO)
At the organisational level, CIIOs are responsible for managing their cybersecurity risks and are the first line defenders and responders.

A core goal of CSA is to strengthen the cybersecurity and resilience of Singapore's CIIs to preserve the provision of essential services while ensuring the benefits of digitalisation remain accessible and reliable. The increasing frequency and prominence of cyberattacks highlight the increasing risk of disruption to essential services, reinforcing the need for extreme vigilance as the risk has never been more prominent.

Global examples demonstrate the extent of the risk

Singapore is not alone in facing this risk. There are prominent examples of such disruption in many countries around the world. The following three examples demonstrate the challenges Singapore faces in securing and maintaining the resilience of essential services in response to cyberattacks:

Colonial Pipeline[4]

In May 2021, the Colonial Pipeline—an American oil pipeline system that originates in Texas and carries approximately 2.5 million barrels per day of gasoline and jet fuel mainly to the south-eastern United States—suffered a ransomware cyberattack that impacted the digitally-connected equipment managing the pipeline. In response to this attack, a decision had to be made to switch the pipeline off for several days while the vulnerability was addressed. This triggered fuel shortages and panic buying, ultimately spiking the price of fuel in affected states.

Ukraine electricity grid[5]

In December 2015, a hacking group compromised the computer systems of three different Ukrainian energy distribution companies, disrupting the national supply of electricity. It is estimated that 30 substations were shut down and that a population of 230,000 people were without electricity for up to six hours.

United Kingdom National Health Service[6]

In May 2017, the WannaCry ransomware infected over 200,000 computers in at least 100 countries. In the United Kingdom, the brunt of the critical impact was experienced by the National Health Service (NHS). Across the NHS network, at least 600 GP and primary care practices reported disruption to services, and over 50 hospitals were unable to access patient records, experienced delays in receiving test results, and were forced to divert patients from emergency departments to other organisations. It is estimated that close to 20,000 patient appointments were cancelled in one week, including for patient surgery and operations.

1.2. Cyber supply chain risk has renewed urgency and focus, catalysed by high-profile attacks

As organisations increase their reliance on digital products and services, they also increase their reliance on the vendors that provide them. The cyber supply chain is a complex, global, and interconnected ecosystem of information, communication, and operational technology products and services.

At the same time, vendors' supply chains continue to become more digitally focused, growing in complexity, breadth and interconnectivity. When an organisation procures technology, it is beyond a simple relationship with a single vendor providing the technology. Instead, organisations connect into the entire extended supply chain ecosystem of vendors, processes, and distributors involved in creating or delivering the technology product or service that is procured. Organisations may be able to understand the cyber risks that emerge when directly engaging with a supplier or the cybersecurity capabilities a vendor must manage those risks.

However, it is difficult to understand the risks introduced by the vendors that a vendor procures from.

A salient feature of many interconnected and complex cyber supply chains of proprietary software products is the large number of code libraries that make up the product but are not managed by the vendor developing the product. Many of these code libraries are open-source, meaning that they are designed to be publicly accessible and available to be viewed, modified, and distributed by any one. It is difficult for organisations to keep track of and have confidence in the level of cybersecurity of these libraries. Additionally, due to the volume of systems that leverage some of the more common libraries, a vulnerability in a library could have an incredibly outsized and devastating effect on potentially billions of systems if it was compromised.

The cyber risks resulting from the cyber supply chain are many and varied, which can include, but are not limited to:

- The risk of disruption of operations to an organisation from a threat actor compromising a technology vendor used by the organisation and leveraging the vendor as a vector into the target organisation

- The risk of disruption to operations of an organisation caused by a critical vendor suffering an outage from a cyberattack

- The risk of threat actors inserting ransomware from malicious software into a technology vendor's product impacting the organisation using the product

- The risk of a data breach of an organisation's confidential information caused by a compromised vendor that processes an organisation's data

Cyber supply chain risks are not new, but threat actors are increasingly exploiting supply chain vulnerabilities. The 2020 Global Incident Response Threat Report from VMWare Carbon Black—a US-based cybersecurity and cloud technology company—found that 55% of cyberattacks occur through supply chains instead of directly targeting the organisation, as unprepared vendors represent a weak link to be exploited and provide a vector to the target organisation[7]. Research by the European Union Agency for Cybersecurity (ENISA) found that close to 62% of supply chain attacks take advantage of the trust that an organisation has in its vendors.

High-profile examples of supply chain cyberattacks have demonstrated the consequences of loss of availability of services and the loss of confidentiality of information. Several major cyberattacks have made the headlines in global news media in 2020 and 2021:

Log4j, is an open-source software provided by the Apache Software Foundation that records system-level events (e.g., errors) and relays diagnostic messages back to users or administrators. In December 2021, a vulnerability was discovered that could lead to threat actors executing malicious code and taking control of servers running the software. The widespread and near-ubiquitous prevalence of Log4j in all kinds of software products makes this vulnerability particularly concerning. The vulnerability has been used by hackers to execute ransomware, mine bitcoin, add servers to botnets and access sensitive government information.[8]

SolarWinds, a US-based technology company that provides network-monitoring and IT administration tools to hundreds of thousands of organisations including Fortune 500 companies and government agencies, had its network breached in March 2020, which allowed hackers to insert malicious code into its popular product Orion. This impacted approximately 18,000 organisations globally, and threat actors accessed sensitive assets and breached the confidentiality of information belonging to various governments, Microsoft, Nvidia, FireEye and others[9].

Kaseya, a provider of software for remote IT monitoring and management, had its systems breached in July 2021. Threat actors were able to remotely execute commands that updated the Kaseya software installed in its customers' networks to deploy ransomware via the compromised software and impact the availability of the customer's business. Of the worst affected, a Swedish retailer, Coop, was forced to shut at least 800 stores for an entire day[10].

The similarity across these three examples is that the attacks were against 'linchpin technologies'—services or products vital to many organisations' functioning. Disruptions to these technologies can create amplified effects that cascade down to have far-reaching impacts. The vendors that provide these technologies are high-value targets for threat actors, as the threat actors can potentially scale the impact of an attack to many of the vendors' customers.

The examples highlighted above demonstrate the impact of supply chain cyberattacks. Highly skilled and persistent, nation-state-backed threat actors, as well as large and well-resourced cybercriminal groups, are increasingly behind supply chain cyberattacks. Of more than 24 high-impact global supply chain cyberattacks reported between January 2020 and July 2021, more than 50% are attributed to well-known Advanced Persistent Threat (APT) groups, often with nation-state backing[11].

A typical supply chain cyberattack has long term objectives of espionage or disruption at its core. The initial access point is often the target organisation's software, cloud, hosting or IT service providers. Using this vector is a sophisticated approach that is indicative of the resources and backing that nation-state-backed groups have at their disposal. The backing

these nation-state-backed groups have enabled these threat actors to plan and execute cyberattacks with significant impact meticulously. Cybercriminal groups also know the benefits of using the supply chain as a vector of attack. The patterns of behaviour of cybercriminals groups are echoing nation-state-backed threat actors.

Supply chains represent one of the most challenging areas for organisations to secure because of the lack of visibility and complete control over the variables that contribute to the risk on the vendors' side. Vendors play an important role in managing these risks for organisations. Vendors manage cyber risks for customers by the cybersecurity practices they put in place to defend their own organisations and products against cyber threats. Methods include mitigating against known vulnerabilities in products and staying vigilant to emerging vulnerabilities. Additionally, vendors are responsible for driving cybersecurity requirements for vendors in the supply chains that make up their products or services and work to mitigate vulnerabilities in the parts or software packages used in their products.

The cyber supply chain is a risk to the organisation that inward-focused cybersecurity controls are unable to address. More companies and regulators are becoming aware of this growing gap and continue to explore viable solutions. This evolving risk necessitates a fundamental shift to develop a sophisticated, forward-looking, multi-layered cyber supply chain resilience approach at the national level to maintain the availability and effectiveness of essential services.

1.3. A foundational programme to improve the resilience of the CII cyber supply chain

The CII Supply Chain Programme ('the Programme') addresses three core objectives towards strengthening the availability and resilience of Singapore's essential services in response to CII cyber supply chain risks:

1 — To develop **a national framework that increases the transparency and visibility of cyber supply chain risks** to CIIs. The framework enables CSA, Sector Leads, and CIIOs to contribute to **effectively managing cyber supply chain risks for CIIs with increasing sophistication**, enhancing the cyber resiliency of Singapore's essential services.

2 — To align a **shared understanding that provides a consistent approach to managing cyber supply chain risks across CIIOs, but flexible to adapt to the needs of different sectors**. This approach drives consistency in how CIIOs assess and **improve the adequacy and efficacy of cybersecurity controls** for information technology (IT), operational technology (OT), and Internet of Things (IoT) products and services vendors used to operate and maintain Singapore's CIIs.

3 — To **catalyse an ecosystem of CIIOs and vendors incentivised to continuously improve cyber supply chain resilience** by establishing the foundational groundwork required to **initiate proper governance structures and drive desired behaviours.**

Resilience for the purposes of this Programme refers to two capabilities – preparedness to identify and protect against cyber threats, and readiness to detect, respond and recover from cyber incidents. The first aspect is identifying the relevant threats, managing the cybersecurity risks and implementing appropriate safeguards to ensure delivery of critical services. The second aspect is improving Singapore's ability to detect incidents quickly, respond faster and more effectively to contain the impact of incidents and recover and restore services from disruption.

The intended benefits and outcomes of the Programme are outlined as follows:

- **A framework to guide CIIOs** in the required practices and processes to increase visibility of CII cyber supply chains, mitigate cyber supply chain risks and improve the cyber resilience of CIIs

- **Enhanced cyber supply chain risk management capabilities** of all CIIOs regardless of sector, current maturity or size

- **Improved CII vendor cybersecurity practices** and the cybersecurity of the products and services they provide

- **Increased collaboration between CIIOs**, especially within individual sectors, to collectively manage cyber supply chain resilience risks in Singapore

- **Reduced information asymmetry** between CII vendors and CIIOs on cyber supply chain incidents to assist with early warning and reduce response and mitigation time

The Programme provides:

1. **A forward-looking programme** to address the core cyber supply chain challenges faced by CSA, Sector Leads, CIIOs and vendors required to reach aspirational resilience goals

2. **An outline of the CII Vendor Management Methodology** and process to use the CII Cyber Supply Chain Assessment toolkit which provides a consistent approach for managing vendors and associated cyber supply chain risks at the CIIO, sectoral, and national level

3. **Guidance to stakeholders** at the organisational, sectoral and national-level on the required roles and responsibilities they should adopt to contribute to improving the resiliency of the cyber supply chain.

Chapter 2: Impetus

2.1. A challenging problem in need of an enhanced and collaborative solution

A broad and representative cross-section of experts from CSA, Sector Leads, CIIOs and industry participated in discussions to understand cyber supply chain resilience trends as they relate to the context of Singapore. In total, all 11 CII Sectors contributed to the shaping of the Programme as well as experts from Singapore, Israel and the United States.

Experts provided valuable information on current practices, pain points, and ambitions for managing cyber supply chain risks within and outside of Singapore. They identified challenges and shortcomings of current approaches used in Singapore.

Three clear challenges have emerged that are common across Singapore:

	Supply chain networks are **global, complex and multifaceted**. It is difficult to understand the **breadth, depth and evolving nature of the supply chain** and manage "known-unknowns" of **cyber and concentration risks hidden amongst complexity**.
	Vendor risk management in Singapore tends to be **compliance-focused, point-in-time and manual.** This is **not sustainable or future-ready** for addressing emerging cyber supply chain risks.
	Sectoral and organisational silos that limits the coordinated action required to collectively manage cyber supply chain risks.

Additionally, the mixed use of OT and IoT for some sectors introduces new industry-specific challenges. Cyber supply chain risk issues differ across sectors depending on the extent of IT, IoT and OT used in each sector.

For OT-predominant sectors, OT systems have long equipment lifecycles and are not easily refreshed or upgraded. Cyber supply chain risks introduced from these systems are difficult to control. Organisations cannot easily switch the equipment to more secure or resilient products or easily change vendors without high costs or disruption. This challenge compounds due to the difficulty to mitigate cyber supply chain risks by implementing patches and controls on these systems which are commonly dispersed and separated across locations. Additionally, OT and IoT systems often require specialised technology with niche vendors that offer a limited choice or the ability to switch to more secure products to reduce cyber supply chain risk.

A common workaround to vulnerabilities in OT systems caused by the cyber supply chain is to remove any connection between the device and the Internet, known as creating an 'air gap'. However, with growing numbers of devices, interconnections and interdependencies between IT and OT, the delineation between OT and IT systems is blurring. Air gaps are no longer sufficient as a control for vulnerable OT systems. More emphasis needs to be placed on vendors to build more secure products or adhere to increased cybersecurity requirements.

For IT-predominant sectors, software permeates through all organisation functions, widening the attack surface that requires protection. Meanwhile, international technology vendors have outsized bargaining power compared to local CIIOs. Structural imbalances mean that CIIOs have limited bargaining power to enforce or customise requirements on vendors without significant cost implications.

Complex and multifaceted supply chains

Complex, multifaceted and interdependent supply chains remain a prominent feature of digitalisation. It introduces new and increased cyber risks to organisations and reducing the ability to control exposure to these risks. An ecosystem of complex, interconnected, and interdependent supply chains limits visibility, transparency or awareness of risks. This creates 'known-unknowns' which introduce systemic cyber risk, impair the transparency for concentration risks and threaten the resilience of cyber supply chains and the CIIOs that derive value from the ecosystem.

The first step to achieve deep supply chain visibility is to focus on immediate vendors. However, there are challenges in achieving completeness of inventories for direct Tier 1 vendors - those vendors for which an organisation has a direct contractual relationship. Furthermore, visibility for each further layer of depth becomes increasingly difficult as the quantity, variety, and complexity of interconnected vendors increases.

Interconnected organisations also present a broad attack surface for exploitation. This situation creates blind spots in cyber supply chains, with vulnerabilities often challenging to detect, creating barriers to awareness and difficulty identifying the systemic cyber risks hidden in the supply chain. There is a need to increase awareness of the potential threats stemming from poor cybersecurity practices of vendors and vendors of vendors.

The complexity of cyber supply chains impairs the transparency of concentration risks affecting linchpin technologies or technology vendors providing highly specialised or niche services or products. Cyber supply chain risk management of linchpin technologies is vital as the impact of disruption from an incident would have an outsized and far-reaching effect on many organisations. Without a national view of CII concentration risks to inform the appropriate mitigating actions, the magnitude of these risks may only emerge when a disruptive incident reveals the extent of reliance on a particular vendor or product.

Risk management processes are not future-ready

Traditional vendor cyber risk management processes focus on the organisation and its direct vendors. Still, this approach is not future-ready to meet the demands of emerging complex cyber supply chain risks constantly evolving in today's multi-layered digital landscape.

Currently, most organisations rely on the following cyber supply chain risk management processes:

- **Performing manual, episodic, point-in-time and compliance-focused cybersecurity assessments of primary vendors.** These methods are often unable to detect new threats and vulnerabilities that emerge in real-time in the complex and opaque cyber supply chain network.

- **Enforcing contractual terms as the primary risk management approach to address vendor cyber risk and resilience**. This reactive approach can negatively impact open information sharing between vendors and CIIOs and potentially motivate vendors to not share valuable incident information promptly.

- **Air-gapping OT and legacy assets to address vulnerabilities, minimise the attack surface and overcome difficulties in patching these assets.** On its own, this approach is no longer sufficient, as IT and OT environments continue to converge, and the boundaries between shared systems and processes blur. This highlights the challenge that today CIIOs are unable to respond in real-time to the changing threat landscape.

Fragmented and siloed approach to cyber supply chain challenges

CIIOs are procuring technology services individually and fail to benefit from combined buying power. The limited leverage over prominent technology vendors and niche vendors means an inability to encourage or enforce enhanced vendor cybersecurity requirements. Vendors are the vector of a supply chain cyberattack on an organisation, and it is their responsibility to mitigate vulnerabilities to prevent incidents. Yet, CIIOs must often balance a procurement trade-off between the cost of services and the level of cybersecurity provided by vendors.

Coordination of cyber supply chain risk management at the sectoral, national and international levels is a real challenge. Collective action for risk management and procurement is limited as CIIOs predominantly manage risks to cyber supply chain resilience in isolation, with sector-level silos not led by national coordination. Forums, governance structures, or incentives to share timely cyber supply chain intelligence, coordinate effective and collective responses to cyber supply chain issues are inadequate to address the increasing challenge. There is limited orchestration at the national level for this wicked problem, indicating missed opportunities to improve efficiency.
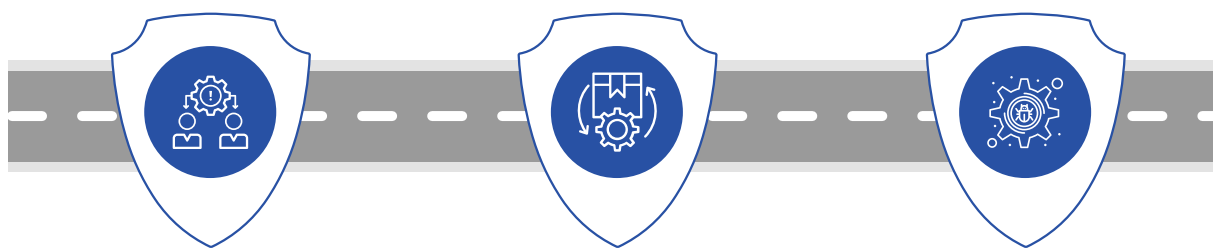
Traditional Cyber Supply Chain Risk Management

- Compliance-focused, checkbox oriented
- One risk assessment, performed before contract signing
- Does not cover entire vendor lifecycle, no additional assessments to capture ongoing risk throughout the lifecycle of the relationship, no vendor off-boarding procedures
- Visibility is limited to large Tier 1 vendors
- Basic set of controls in place for managing risks, limited resources to assess risks at deeper tiers and limited ability to influence decisions beyond Tier 1
- Process conducted by individual CIIOs, limited information sharing between CIIOs or sectors
- Does not consider criticality/resilience requirements of assets/services, misaligning risk management efforts to areas that do not offer the most value

Changes to the Structure of Cyber Supply Chains

- Velocity of changes in supply chains and threats have increased, yearly checks are soon out of date
- More risks emerging from deeper into the supply chain (Tier 2, 3, 4…N), than Tier 1, but visibility is harder to achieve as supply chains become more complex

New Requirements to Achieve Cyber Resilience

- Focus on resilience, linked to the criticality of assets or services
- End-to-end cyber supply chain risk management including monitoring of cyber risks with focus on incident response and recovery in the event of a cyber incident
- Increased collaboration among CIIOs within a CII sector and across sectors
- Increased collaboration between critical vendors to improve cybersecurity controls and incident response coordination (including conducting incident response and disaster recovery exercises)
- Visibility to the nth tier of the supply chain

Chapter 3: Key Principles for CII Cyber Supply Chain Resilience

To address the key challenges for Singapore's cyber supply chain resilience highlighted in the previous chapter, CSA has developed the CII Supply Chain Programme to offer a practical, achievable approach for resilience, that is both fit-for-purpose and promotes sound practice.

There are five principles that guide the direction of the approach described in Chapter 4, including both scope and actions required to facilitate change.

Living blueprint

The Programme is a living blueprint that continues to evolve and adapt to tackle changing risks.

Multi-stakeholder oriented

The Programme involves stakeholders across all layers of CII responsibilities to develop a holistic solution.

Ecosystem driven

The Programme promotes an ecosystem of partnerships driven by reasonable incentives to encourage the desired behaviours and of stakeholders.

Transparent and open standards

The Programme uses available risk management standards and sound practices, striving for consistency and avoiding duplication of successful existing frameworks.

Proactive and continuous risk management

The Programme promotes proactive and continuous risk management through the vendor lifecycle to move beyond a checkbox mentality.

3.1. A living blueprint

The Programme constitutes a living blueprint that continues to evolve, providing an agile approach to address emerging threats and changing risks over time.

The Programme is flexible, customisable, and continuously refreshed to meet the ever-changing demands across different sectors. It can accommodate the various needs of diverse sectors (i.e., Sector Leads and CIIOs from different sectors) and stay current in the face of the rapid pace of change in the technology landscape.

The specificity of the framework calibrates the needs of CIIOs at each layer in the cyber supply chain ecosystem. Delivery and implementation of initiatives will require specificity and detail of standards and procedures to be adapted to a CIIO's operating situation and industry. Still, the fundamental principles and goals flow from the top (i.e., national or sector level), with the right amount of flexibility across sectors.

Flexibility and agility are also essential to accommodate and adapt to the rapid pace of technology change. The Programme avoids overly prescriptive guidance, standards, or procedures as they may soon become obsolete and hinder efforts by industry to adopt improved solutions that push against existing advice in the future.

Hence, the focus is on using risk management principles and assessment standards (e.g., essential characteristics, actions, or processes) rather than creating standards concentrated on specific technologies or methodologies.

3.2. Multi-stakeholder oriented

Risks to cyber resilience in the supply chain do not exist in a vacuum. They are complex and cascade across multiple parties. Activities undertaken to address the cyber supply chain challenges consider how to facilitate collaboration between all concerned stakeholders.

The Programme involves stakeholders across all layers of the cyber supply chain ecosystem to develop a holistic solution. CSA as the national agency and regulator for CIIs is best placed to drive key initiatives for cyber supply chain resilience at the national level. Sector Leads who are statutory boards with supervisory or regulatory responsibility over an industry or sector to which the CIIO is best placed to guide uptake of key initiatives at the sector level. CIIOs and vendors collaborate to deliver and protect the CIIs that deliver essential services.

Successful organisations manage cyber supply chain risks in multi-disciplinary and collaborative ways. The Programme considers the variety of levers that each stakeholder group has available to address challenges and the opportunities for different parties to work together.

3.3. Ecosystem driven

Progressing towards the desired cyber resilience goals for the cyber supply chain ecosystem through directives, standards, collaboration, and communication structures will be ineffective without motivating or influencing stakeholders to enact the desired behaviours and partnerships.

The Programme considers foundational initiatives leading towards a cyber supply chain ecosystem where the market incentivises vendors to embed desired behaviours and create mutually beneficial partnerships with CIIOs. This would help vendors to:

- **Demonstrate compliance** to requirements and encourage accountability for cybersecurity

- **Boost consumer confidence** in a vendor's management of cybersecurity practices, handling of personal data and availability of services

- **Promote consistency** in standards across sectors

One area for consideration is regular public-private consultations and partnerships at various levels (national, sectoral and organisational). This could include placing cyber supply chain risks on the agenda of high-level government business talks or forums, a vertical public-private task force for the development of new frameworks and tools, organising public conferences for the sharing of mitigation means, tools and techniques, or confidential consultations with specific companies or sectors.

However, vendors and CIIOs may have concerns that hinder voluntary disclosure of cybersecurity vulnerabilities in the supply chain.

For vendors, these concerns are:

- Impacts on competitive advantage

- Implications on contractual terms-of-service from disclosing a vulnerability to a customer before resolution

- Implications of liability from a vulnerability leading to an incident that affects a customer

For CIIOs, these concerns are:

- Regulatory sanction or financial penalties resulting from an incident caused by a known vulnerability

- Negative impacts on the economic value of the CIIO due to the market perceiving negligence, inaction or inability to fix a vulnerability

There is a need to address the concerns of vendors and CIIOs by establishing trust-building mechanisms into regulations and contracts such as anti-competition exemption, restrictions on sharing and use of information, protection from liability, and proprietary information protection.

Another opportunity is to use Sector Leads or other regulatory levers to promote certification of products or vendors. Certification could signal to CIIOs that a vendor has taken cybersecurity (specifically as it pertains to its cyber supply chain) into account.

A downstream effect of creating an environment of engaged stakeholders in the cyber supply chain ecosystem is that a critical mass of leading CIIOs become actively engaged in the topic of cyber supply chain resilience and thus more accountable for their actions. Advocacy, influence and engagement in the ecosystem help to generate continuous momentum towards improved resiliency of the cyber supply chain.

3.4. Transparent and open standards and sound practices

The Programme leverages transparent and consistent standards and sound practices to define initiatives and requirements. Leveraging existing industry-recognised standards such as the ISO 27001 standard and NIST Cybersecurity Framework leads to convergence on a common set of requirements aligned to sound practices that are established and widely known to many organisations to incentivise CIIOs to implement. With standardised cyber supply chain risk management practices, CIIOs can more effectively integrate requirements of the Programme or future cyber supply chain initiatives with existing risk management processes.

The Programme considers alignments with other countries and regulatory bodies to create international consistency as to what to expect of vendors and facilitate smooth information sharing, coordination, and collaboration now and in the future with international counterparts.

A standardised framework that 'speaks a common language' helps buyers build trust in their vendors, as the transparency enables buyers to understand the vendors' commitments to their cybersecurity position. Vendors can provide information on their cybersecurity capabilities that is consistent with other vendors, so buyers can understand the information that is being provided. Buyers can also know what requirements should be in place, and what information to ask for.

3.5. Proactive and continuous risk management

The Programme emphasises an approach to cyber supply chain risk management that is proactive and continuous throughout the vendor lifecycle. This approach encourages CSA, Sector Leads and CIIOs to take ongoing preventive measures to assess and prevent cyber supply chain risks.

The Programme pushes CIIOs to pivot towards anticipating and mitigating cyber supply chain risks continuously. Monitoring and addressing gaps in vendor cybersecurity controls can no longer take a point-in-time approach; it needs continuous assessment and tracking.

The Programme outlines cyber supply chain risk management as a process that continues across the entire vendor lifecycle. The Programme guides CIIOs to direct efforts to assess risks during procurement, perform periodic reassessment throughout the time the vendor is engaged, and manage the risks from decommissioning vendors.

The Programme also encourages vendors to be involved in incident response planning and simulation exercises alongside CIIOs, Sector Leads and CSA to strengthen Singapore's ability to detect and respond to cybersecurity incidents.

Chapter 4: A Programme to Improve CII Cyber Supply Chain Resilience

To address the challenges of the complexity of hyperconnected and multifaceted supply chains in our modern landscape, a fundamentally different approach to cyber supply chain risk management must be adopted by Sector Leads, CIIOs and vendors as defined in the Programme outlined in this paper.

The Programme includes comprehensive updates to cyber supply chain risk management processes to nurture a system that proactively responds to emerging, high-velocity risks. It provides unified and standardised approaches to cyber supply chain resilience for all CIIs, to underpin and enable collaborative and collective actions for a more resilient national ecosystem.

Current Scenario		Ambition
Limited oversight, lacking a clear understanding of relationships between CIIs and vendors	›	Detailed **inventory of all Tier 1 vendors** of CII assets, ability to **push to nth Tier** for high-risk vendors
Limited visibility of risks, and difficulty distinguishing types of risks across different vendors	›	Multi-factor risk identification, with a **nuanced understanding of different risk types and levels** (e.g., critical, concentrated or systemic vendors)
Limited **point-in-time assessments**, usually during initial onboarding or procurement	›	Regular assessments as part of a **continuous monitoring process, with regular analysis of vendor inventory and risks** for both new and existing vendors
Compliance-focused response, **often a tick-box exercise** performed and managed by IT departments in silos	›	**Resilience-focused assessment** as part of proactive approach incorporating multiple departments, including Board of Directors
Barriers to incident information sharing and collective cyber supply chain incident response between CIIOs and vendors	›	**Collaborative cyber supply chain incident response** between CIIOs and vendors including cross-sector collaboration

The Programme is a guiding roadmap for CII stakeholders to address a wide range of cyber supply chain challenges and achieve a desired state of resilience by developing foundational enablers of a secure and fit-for-purpose cyber supply chain resilience approach. This ambition is for:

- **Transparency.** Visibility of cyber supply chain risks across CIIs.

- **Standardisation.** Common language and a consistent approach to cyber supply chain risk management.

- **Incentivisation.** Catalysing an ecosystem of CIIOs, vendors, government agencies, and regulators motivated to improve cyber supply chain resilience.

This approach is practicable, actionable, and flexible to address today's cyber supply chain risk challenges while providing a framework to adapt to changing future needs, it:

- **Aligns** with recognised principles

- **Focuses** on high-impact intervention

- **Ensures** feasibility of implementation

- **Establishes and maintains** appropriate control over the end-to-end cyber supply chain

4.1. Scope of the Programme

The complex nature of the ecosystem means there is no one-size-fits-all method to definitively capture and define what the cyber supply chain is and what the focus of visibility, control, risk management and resilience in the Programme should be.

Breadth and depth are two primary variables that bound the extent of the cyber supply chain and focus on the scope of the Programme. Breadth addresses the inclusion of different types of vendors, services, or products into the cyber supply chain. Depth addresses the degree of depth of vendor tier to include in the cyber supply chain.

There is no simple choice for how deep or wide the focus of the cyber supply chain should be in the Programme to achieve effective risk management and enhanced resilience. The realities of the risk landscape further complicate these choices.

Cyber risks can be present at any layer in the supply chain, often creating assessment needs that can be burdensome. Focusing only on third-party vendors may miss out on crucial risks at deeper levels of the cyber supply chain, as the vendors of vendors may introduce potential vulnerabilities. However, gaining visibility into the cyber supply chain's deeper layers is incredibly challenging as it creates a complex assessment process for CIIOs to manage.

Non-technology vendors may also introduce cyber supply chain risks. These vendors do not actively provide technology products, but the nature of interconnected ecosystems means that they may still introduce vulnerabilities into the cyber supply chain. Introducing these vendors into the scope of the Programme, however, will dilute efforts to gain visibility of the vendors who are most likely to introduce cyber risks, which is a goal of the Programme.
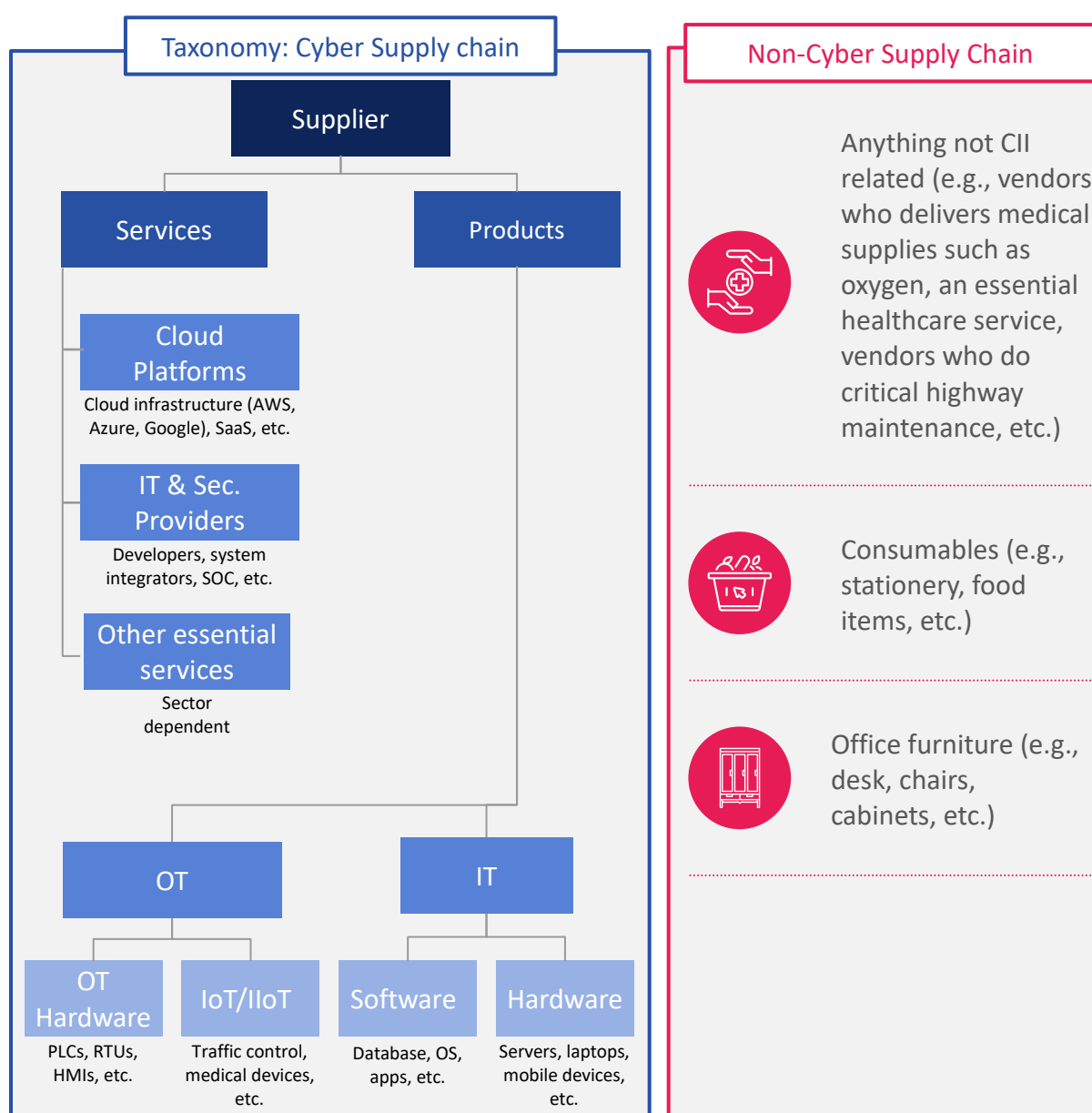
Incidents within the deeper layers of supply chains can cause ripple effects with lasting impacts for CIIOs. The impact of an adverse incident is even more significant when it occurs to critical Tier 1 vendors. However, the avenues of control to mitigate impacts in the deeper

layers of the supply chain are far less practicable. They often require a significant investment of resources that deliver decreasing returns.

The scope of the cyber supply chain in this Programme is defined based on factors of visibility and practicality to keep the scope of vendors manageable and effective:

- **Visibility.** What level of breadth and depth is right to identify the relevant risks in the supply chain?

- **Practicality.** What is the cost required to reach the required level of visibility and how does it balance improvements to cyber supply chain resilience with other priorities? What practical actions to improve cybersecurity could a CIIO take with that level of visibility?

4.1.1. Breadth

layers of the supply chain are far less practicable. They often require a significant investment of resources that deliver decreasing returns.

The scope of the cyber supply chain in this Programme is defined based on factors of visibility and practicality to keep the scope of vendors manageable and effective:

- **Visibility.** What level of breadth and depth is right to identify the relevant risks in the supply chain?

- **Practicality.** What is the cost required to reach the required level of visibility and how does it balance improvements to cyber supply chain resilience with other priorities? What practical actions to improve cybersecurity could a CIIO take with that level of visibility?

4.1.1. Breadth

Taxonomy: Cyber Supply chain

Supplier
- Services
  - Cloud Platforms — Cloud infrastructure (AWS, Azure, Google), SaaS, etc.
  - IT & Sec. Providers — Developers, system integrators, SOC, etc.
  - Other essential services — Sector dependent
- Products
  - OT
    - OT Hardware — PLCs, RTUs, HMIs, etc.
    - IoT/IIoT — Traffic control, medical devices, etc.
  - IT
    - Software — Database, OS, apps, etc.
    - Hardware — Servers, laptops, mobile devices, etc.

Non-Cyber Supply Chain

- Anything not CII related (e.g., vendors who delivers medical supplies such as oxygen, an essential healthcare service, vendors who do critical highway maintenance, etc.)

- Consumables (e.g., stationery, food items, etc.)

- Office furniture (e.g., desk, chairs, cabinets, etc.)

This Programme focuses on the OT and IT assets within CII perimeter boundaries. The breadth of the cyber supply chain scope includes vendors that provide products and services to CII assets and introduce potential cyber risks.

A CII is a computer or computer system(s) directly involved and necessary for the provision of and continued delivery of an essential service. An essential service is defined by each Sector Lead and CSA and is governed by the Cybersecurity Act 2018. The Programme applies to all services and products leveraged by a CIIO to facilitate the operations of CIIs.

In-scope	NOT in-scope
Examples of vendors who **ARE** within scope of the foundational stages of the Programme include, but are not limited to:	Example vendors who **ARE NOT** within scope of the foundational stages of the Programme include, but are not limited to:
IT and cybersecurity service providers	Providers of consumables (e.g., stationery, catering, food)
Telecommunications service providers	Office furniture (e.g., desks, chairs, cabinets)
Cloud platforms	Contractors and service providers who do not deliver a service directly related to the CII (e.g., building management system vendor for the office of a CIIO)
OT hardware products	
IoT/IIOT hardware products	
IT hardware products (e.g., firewalls, computers, mobile devices)	
IT software products (e.g., enterprise software, cybersecurity software, database technologies, operating systems)	

4.1.2. Depth

Shallow   Deep

Step 1: Ringfence to Tier 1	Step 2: Prioritise vendors via risk-based approach	Step 3: To the Nth tier
Start with a contained scope – define a comprehensive inventory across Tier 1 including the entire CII lifecycle from design, implementation, to maintenance	**Move to a manageable scope –** naturally tapers off scope to T3 or T4 suppliers with clear links between them **Managed effort –** break down a large supply chain of interdependent vendors using prioritisation based on cyber risk rating and the risk appetite of the organisation **Visibility of common risks –** code manipulation in a supplier product, hardware counterfeits, poor supplier software development practices, or access to a network or data are most common vectors for supply chain cyberattacks and highest priority to manage **Increased resiliency –** appropriate 80/20 level of mitigation and response efforts for cyber supply chain risks, addressing the objectives of the Programme	**High visibility of risks –** ability to detect ripple effects from systemic cyber risks plus other supply chain risks

In Section 4.1.1, the breadth of scope captures the vendors capable of introducing the highest impact risks and most common supply chain cyberattack vectors to CIIs. The breadth maps all direct material vendors within the CII perimeter boundary, which we define as Tier 1 vendors.

However, a wide variety of complex cyber supply chain risks exist at Tiers beyond Tier 1. It is important for CIIOs, and Singapore's ecosystem, to enhance the visibility of vendors in the cyber supply chain towards the nth Tier (the deepest Tier in the supply chain).

Improving transparency of the risks hidden at the nth Tier allows CIIOs to identify relevant risks and implement effective control measures to mitigate against adverse impacts. However, CIIOs and sectors are at varying points on their cyber supply chain risk management journeys. Achieving n^{th} Tier visibility of the supply chain is challenging and costly and requires an approach that reflects the differing starting points of respective CIIOs.

This Programme views n^{th} Tier visibility as an aspirational goal for CIIOs, but foundational at the national level. It seeks to guide CIIOs to achieve visibility at the furthest practicable depth of the supply chain by following a clear set of risk management principles:

- Align risk management with organisational goals
- Align risk mitigation to risk appetite
- Reduce the cost of mitigation over time
- Adopt a continuous iterative process

When a centralised view of nth Tier CII vendors is achieved, there is potential to map out the different functions of the supply chain at the national and sectoral level. CSA and Sector Leads can use this view to define the criticality and risks associated with cybersecurity and vendor concentration. They can then develop national and sector level initiatives to address these risks directly.

4.2. The role to be played by ecosystem stakeholders

Effectively managing risks in the cyber supply chain requires a multi-stakeholder effort. It involves a range of stakeholders engaged and actively playing a part across government, Sector Leads, CIIOs, and vendors.

Stakeholders are in a solid position to take individual action but acting in isolation is not an effective way to solve challenges and ensure resiliency across the ecosystem. Collaboration between parties is required to better manage risks to supply chain resilience and contribute to a secure national landscape. Managing this landscape requires new initiatives to incentivise the adoption of cyber supply chain security practices and hold stakeholders accountable for cybersecurity and resilience outcomes.

This Programme is a call-to-action for all stakeholders to contribute and play their part and work towards identifying opportunities to enhance the resilience of the cyber supply chain:

- CSA is the national agency and regulator **driving, orchestrating and championing national cyber supply chain resilience**, working with stakeholders to identify opportunities and facilitate successful initiatives between relevant groups, public and private

- Sector Leads are statutory boards, **driving supply chain resilience within their respective sectors**, guiding CIIOs to improve resilience capabilities while considering sector-specific requirements and trade-offs

- CIIOs are the **legal owners of their CIIs**, working collectively with CSA, Sector Leads, and vendors to create a mutually beneficial ecosystem that improves cyber supply chain resilience

- Vendors contribute to the ecosystem by **maintaining strong and transparent relationships with CIIOs** and maintaining the cybersecurity and resiliency of their organisation and services or products.

This Programme sets out the expected roles and responsibilities that each stakeholder plays in contributing to a vibrant ecosystem that unlocks the value of technology while strengthening the resilience and cybersecurity of cyber supply chains in Singapore. The key initiatives consider the specific responsibilities required of each group of stakeholders.

4.3. Key Initiatives

In consultation with experts and CII stakeholders, the Programme outlines practical and impactful initiatives to achieve the ambitions outlined in the Programme and address the challenges of cyber supply chain resilience in Singapore. The initiatives are derived from a framework that focuses on five mechanisms of actions across the different layers of CII stakeholders. Initiatives were stress-tested and down-selected by considering comparisons with benchmarks from leading countries, their ability to address the defined challenges that lead to the required outcomes and address the stakeholder's pain points, and the feasibility of implementation.

	Organisation Level	Sector Level	National Level	International Level
1 Legislative Guidelines	*Establish regulatory guidelines drives accountability for stakeholders to manage cyber supply chain risk*			
2 Tools & Technology	*Develop new technology tools and platforms to assist in managing cyber supply chain risk*			
3 Ecosystem Development	*Encourage collaboration through a national and global cybersecurity ecosystem*			
4 Market Incentives	*Use of market forces incentivise vendors to improve their baseline cybersecurity practices*			
5 Education	*Improve situational awareness and change attitudes among executive leadership and business functions*			
	Maintenance of essential services of CIIs	Enhancing resiliency of essential services in respective sectors	Enhancing the resiliency of essential services for the whole of Singapore	Enhancing international cooperation to drive a global view
	Collaborate cross-department within CIIO, and collaborate with other CIIOs within respective sectors	Create collaboration opportunities and partnerships between CIIOs within respective sectors	Create collaboration opportunities and partnerships between sectors	Create collaboration opportunities between countries

Completing the following five key initiatives sets the foundation to achieve the target state ambition:

Initiative 1: CII Cyber Supply Chain Assessment Toolkit

A vendor management methodology and data model to generate nth level visibility of the critical infrastructure cyber supply chain at the national level. Standardises a national methodology for CII cyber supply chain risk management and improving line of sight into CII cyber supply chains and transparency of risks.

Initiative 2: Cyber Contractual Handbook for CIIs

A centralised service for CIIOs to access a repository of sound contractual terms and specialist advice for enforcing cybersecurity standards in vendor contracts. Improves the negotiation power of CIIOs over vendors to enforce baseline cybersecurity practices.

Initiative 3: Vendor Certification Programme

A programme that provides the foundational efforts to incentivise vendors to uplift their cybersecurity capabilities and recognise vendors who have achieved cybersecurity standards and certification.

Initiative 4: Cyber Supply Chain Learning Hub

A platform for cross-functional knowledge sharing and training resources for critical infrastructure owner stakeholders. Improves awareness and appreciation of cyber supply chain risks to drive uptake of key initiatives and encourages uptake of sound practice cyber supply chain risk management at CIIOs and vendor organisations.

Initiative 5: International Cooperation

An expansion of activities internationally to develop global information sharing forums, engage in global cyber supply chain capacity-building and interoperable standards and certification. Expands the reach of Singapore's position in cyber supply chain resilience and improves capabilities of cyber supply chain risk management.

Key initiatives for enhanced national CII cyber supply chain resilience

1   **Cyber Supply Chain Assessment Toolkit**

- **Standardised methodology** and framework for CII cyber supply chain risk management and assessment
- **A data-driven model to increase visibility** to n^{th} Tier vendors
- **Accurate, up to date and real-time analysis** of vendor risk data

2   **Cyber Contractual Handbook for CIIs**

- **Transparent sharing of sound cybersecurity contractual clauses** for CIIOs to leverage
- **Greater negotiation power** over vendors for baseline cybersecurity requirements
- **Living document** refreshed by CSA after feedback from CIIs

3   **Vendor Certification Programme**

- **Baseline cybersecurity hygiene** of CII vendors aligned to a **national standard**
- **Curated set of certifications and standards** to uplift cyber hygiene and increase level of trust between vendors and organisations
- **Industry-specific requirements** added on to curated set of certifications and standards to **address uniqueness of each sector**

4   **Cyber Supply Chain Learning Hub**

- **Online learning hub with curated content covering up to date sound practices** and emerging risks for a wide variety of stakeholder types
- **Training and awareness packages** for direct training programmes to CII stakeholders

5   **International Cooperation**

- **Develop close collaborations and working relationship** with international partners to tackle cyber supply chain resilience challenges and build collective capacity
- **Information sharing forums, interoperable standards and mutual recognition**

Chapter 5: Cyber Supply Chain Assessment Toolkit

An initial step towards increased cyber supply chain resilience is to increase the depth and completeness of visibility of vendors in the CII cyber supply chain at the national level and standardise the process of cyber supply chain risk management for CIIOs. Reaching this outcome requires a shared toolkit that unites CSA, Sector Leads and CIIOs under a single framework for cyber risk management and collects the necessary data to achieve nth Tier visibility of vendors in the CII cyber supply chain.

5.1. The challenge to overcome: cyber supply chain risks are hidden amongst complexity

As described in previous chapters, the CII supply chain is complex, interconnected and multifaceted. CIIOs have varying levels of visibility of the cyber supply chains that make up their CIIs and manage the associated vendor risks independently using different approaches. As such, there is low visibility of CII cyber supply chain risks at the national level. This limited visibility translates to a reduced situational awareness of national supply chain risks possibly leading to an ineffective response to a potential incident.

Cyber supply chain risk correlates with decreased visibility of how procured technology by the CIIOs is developed, sourced, integrated and deployed. Managing this risk without visibility of the vendors that make up the supply chain is a case of working with "known-unknowns". Compounding the visibility issue is that risks lie deeper in the supply chain, beyond Tier 1. There are varying levels of completeness of inventories of Tier 1 CII vendors and limited line-of-sight into the CII vendor landscape that is needed to know which vendor relationships to manage more closely. Without a clear picture of the Tier 1 vendor landscape, it is difficult to gain any further visibility beyond this point.

At the same time, identification of the criticality of vendors and vendor risks are in silos. Varied and non-standardised practices are used to calculate and analyse exposure to cyber supply chain risks across sectors. This lack of uniformity makes it difficult to consistently measure and understand risks across different CIIs, CIIOs and sectors.

Additionally, this variation in approach across CIIOs and sectors extends to assessing and rating vendor cybersecurity capabilities. It is essential to understand the processes, procedures, and practices that vendors have in place to manage the cybersecurity and resilience of their organisation and the quality and integrity of the products and services they provide. Without a consistent approach to assessing and measuring vendor cybersecurity capabilities, it is challenging to standardise requirements on CII vendors to manage identified risks or develop the appropriate mitigating controls for CIIOs.
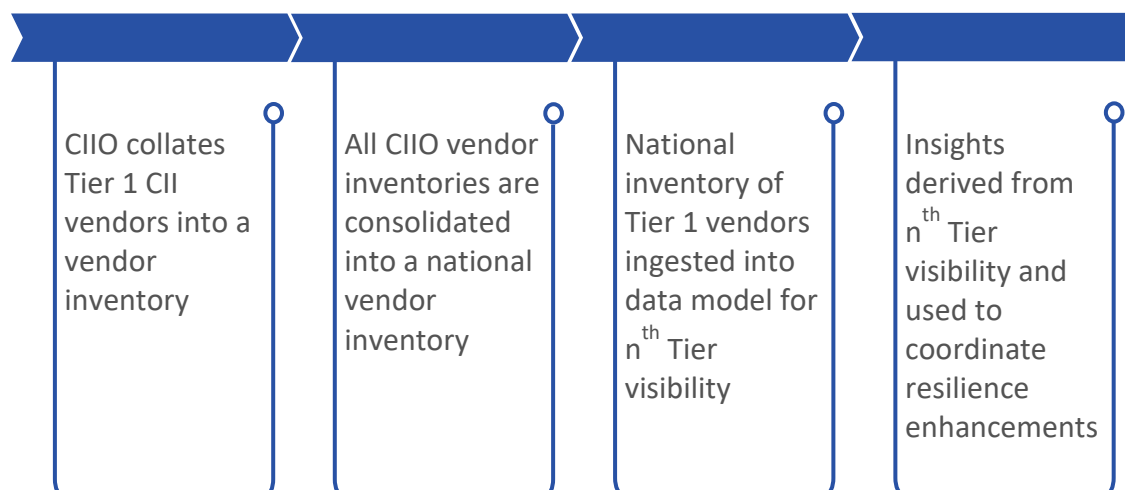
With a limited, varied and siloed approach to cyber supply chain visibility at the organisational and sectoral level, there are challenges to developing a national view of CII vendors, CII cyber supply chain risks or CII vendor cybersecurity capabilities. Without national visibility of the CII cyber supply chain and a centralised view of CII concentration risks, CSA is limited in the collective effort it can take to assist sectors and CIIOs in improving the resilience of the cyber supply chain. This can also hamper efforts to assist CIIOs in quickly identifying the blast radius and coordinating a national response from a supply chain incident.

5.2. The approach: a toolkit to improve cyber supply chain visibility

The CII Cyber Supply Chain Assessment Toolkit (the 'Toolkit') improves the line-of-sight of CII vendors towards n^{th} Tier visibility. It standardises a cyber supply chain risk management approach that is consistent for CSA, Sector Leads, CIIOs and vendors.

The Toolkit consists of four parts:

- **A standardised vendor management methodology** for CIIOs (outlined in Technical Appendix A)

- **A toolkit for CIIOs to collate a Tier 1 CII vendor inventory** with associated assessment questionnaires, risk scoring logic and dashboards

- **A tool for sustainable storage**, maintenance and updates of vendor data

- **Subsequent data-driven model that provides nth Tier visibility of** the entire CII cyber supply chain nationally and real-time cyber risk insights

CIIO collates Tier 1 CII vendors into a vendor inventory	All CIIO vendor inventories are consolidated into a national vendor inventory	National inventory of Tier 1 vendors ingested into data model for n^{th} Tier visibility	Insights derived from n^{th} Tier visibility and used to coordinate resilience enhancements

The Vendor Management Methodology defines a multi-step process for CIIOs to assess, monitor and manage cyber risks of their Tier 1 CII vendors across the vendor lifecycle. Technical Appendix A describes the complete details of this process, and the methodology necessitates CIIOs to perform the following activities:

- **Identify all Tier 1 vendors** used to deliver CII assets and log them in a centralised inventory

- **Assess the importance of individual vendors** to the continuation of the overall operations of a CII

- **Assess the baseline cybersecurity maturity of individual vendors** through a toolkit covering various cybersecurity categories

- **Assign each vendor a risk score** based on importance and maturity

With many CII vendors and technology landscapes in constant flux, manually updating and maintaining completeness and correctness of the inventory in a simple template is not sustainable long-term. A robust tooling capable of automating data collection and updating entries in real-time provides an option to host the national inventory and ongoing inputs and updates to the vendor data by CIIOs and Sector Leads.

The list of Tier 1 CII vendors can be input into a data-driven model that maps the visibility of the cyber supply chain to the nth Tier. With n^{th} Tier mapping, the risks deep in the cyber supply chain can be analysed at the national level to detect concentration risks, potential cascades of follow-on impact, and an incident's potential blast radius. With access to these insights, CSA can facilitate centralised and coordinated support to Sector Leads and CIIOs for mitigation or incident response.

A data-driven cyber supply chain model allows the ability to monitor, alert, analyse incidents in real-time and model the effect of scenarios in real-time. Automated real-time insights for the entire CII supply chain allow CSA, Sector Leads and CIIOs to take highly targeted actions in managing cyber supply chain risks at a quicker pace not available under the previous paradigm of decreased visibility.

5.3. The benefits of improved visibility

The Toolkit provides clear actionable benefits to CSA, Sector Leads, CIIOs and vendors, including:

- Standard approach and requirements for CIIOs to identify vendors and assess cyber supply chain risks

- Consistent set of information required by vendors to answer maturity assessment questionnaires

- Complete data set of Tier 1 CII vendors aggregated at the national and sectoral level, providing a launching pad for CSA and Sector Leads to perform collective action and further initiatives in this Programme

- Visibility of the CII cyber supply chain to the nth Tier, revealing risks previously hidden by complexity and obscurity

- Potential real-time monitoring of risks and incidents for improved response speed and more effective actions

5.4. The role to be played by CII stakeholders

CSA

Role	Champion the Toolkit and orchestrate data collection, maintain the central data source and drive national initiatives developed from Toolkit insights
Responsibilities	- Set the direction for strengthening the security and resilience of CII and its supply chains based on insights from data collected in the Toolkit - Drive the use of the Toolkit and establish mechanisms to ensure uptake and effectiveness - Guide Sector Leads and CIIOs on how to implement the Toolkit in their sector and organisation - Maintain line-of-sight of all Tier 1 vendors providing services for CIIs and use this to generate nth Tier visibility of the CII cyber supply chain - Monitor risk dashboards in the Toolkit and identify areas for improvement or risk mitigation

Sector Lead

Role	Champion use of the Toolkit within its sector, collate sector level CII vendor data and share with CSA
Responsibilities	• Leverage the Toolkit to identify vendor cyber supply chain risks and vendor concentration risks in its sector • Collect, track, and share data collected from the Toolkit to CSA • Collaborate with CSA and CIIOs on creating effective guidance and rules to improve uptake of the Toolkit

CIIO

Role	Use the Toolkit to collect data from CII vendors, work collectively with CSA, Sector Leads, and vendors to develop a complete picture of CII vendors
Responsibilities	• Collect data and complete questionnaires for all Tier 1 CII vendors • Use the Toolkit to manage vendor cybersecurity risks in its organisation • Share information collected in the Toolkit to Sector Leads and CSA • Collaborate with other CIIOs in its industry to manage industry-specific risks and share information • Develop mutually beneficial relationships with vendors that incorporate cybersecurity as a central tenet of the relationship

Vendor

Role	Provide technology for CIIs, maintain strong and transparent relationships with CIIOs and provide information to CIIOs to complete risk management questionnaires
Responsibilities	• Develop mutually beneficial and transparent relationships with CIIOs that incorporate cybersecurity as a central tenet of the relationship • Provide information to CIIOs required to complete maturity assessment questions in the Toolkit • Maintain security controls and conduct regular assurance activities to ensure continued compliance with security requirements of CIIOs and CSA

Chapter 6: Cyber Contractual Handbook for CIIs

The Cyber Contractual Handbook (the 'Handbook') is a centralised service for CIIOs to access a repository of sound contractual terms for enforcing cybersecurity standards in vendor agreements that assists CIIOs in managing vendor contracts across the vendor lifecycle. The Handbook delivers transparent, open information sharing and collaboration between CIIOs, reducing the information asymmetry between vendors and CIIOs to level the playing field during contract negotiations. Simultaneously the Handbook increases efficiency for vendors serving CIIOs as it simplifies the contracting process by standardising controls and consistency of cyber contractual clauses.

6.1. The challenge to overcome: information asymmetry and market power of vendors

CIIOs vary in size and cybersecurity capabilities. For CIIOs which are more established and matured in their respective industries, they are more likely to be able to negotiate for more stringent contractual clauses for enforcing cybersecurity standards in their vendor agreements. For CIIOs which are smaller in market size and less matured, they may not have access to these sound contractual clauses or unable to influence vendors for addition of more stringent contractual clauses.

Additionally, there is an uneven playing field between vendors and CIIOs during contracting. As prominent technology vendors or niche providers have more market power than their CIIO purchasers, CIIOs are unable to create leverage to enforce cybersecurity contractual clauses due to the lack of purchasing power and limited vendor alternatives.

Vendors' information asymmetry when negotiating contracts can be reduced if there is a process to share best practice contractual clauses for cybersecurity standards among the CIIOs. CIIOs have an opportunity to use the information to influence and negotiate for improved cybersecurity standards of vendors collectively.

6.2. The approach: Holistic management of cyber supply chain risks through cybersecurity contractual terms

The Handbook is a living document for two-way information exchange to take place between CSA, Sector Leads and CIIOs to share inputs on the clauses and consolidation of Sector Leads' and CIIOs' feedback and experiences.

Information sharing and exchange can be facilitated through various channels, such as forums and consultation sessions with Sector Leads and CIIOs. From the information gathered, coupled with the insights from the CII Cyber Supply Chain Assessment Toolkit, CSA can form a holistic view of the approach CIIOs are taking to address cyber supply chain risks through contractual terms. This view can lead to insights into the varying capabilities of CII vendors and the challenges that CIIOs have in negotiating with CII vendors and enforcing cyber contractual terms.

The outcome of this holistic view is to progress towards the development of a set of sound practice contractual terms that define control requirements for CII vendors and align to the control requirements in the Cybersecurity Code of Practice (CCoP). The CCoP is issued by the Commissioner of Cybersecurity for the regulation of owners of CII in accordance with the Cybersecurity Act. It is intended to specify the mandatory minimum protection policies that a CIIO shall implement to ensure the cybersecurity of its CII.

A central repository hosts the contractual terms on common cybersecurity risks, operational risks and challenges in contracting with vendors. CIIOs can then use the information to guide contract negotiations for new vendors or when refreshing existing vendor contracts.

6.3. The benefits of transparently sharing contractual clauses

The Handbook provides clear and actionable benefits to CSA, Sector Leads, CIIOs and vendors, including:

- Reducing information asymmetry of vendors to CIIOs and increasing CIIO negotiation power by transparently sharing contractual clauses amongst CIIOs

- Improving cybersecurity capabilities of CIIOs by transparently sharing actionable best practices and contractual terms

- Raising the standard of vendor cybersecurity practices by CIIOs setting a collective baseline in contractual control requirements and placing collective pressure as leverage to negotiate with vendors to reach this standard

- Shifting the culture of CIIOs towards collaboration by improving the transparency of CII cyber supply chain risk management practices

- Increasing efficiency of contractual processes for both CIIOs and vendors by standardising clauses and agreements.

6.4. The role to be played by CII stakeholders

CSA

Role	Champion uptake of the Handbook and orchestrate its creation, maintain a repository to collate and openly share sound practice contractual clauses and guidance for cybersecurity in vendor contracts to CIIOs
Responsibilities	• Collaborate with international groups and counterparts in other countries to facilitate information sharing on sound practices for including cybersecurity clauses in vendor contracts • Facilitate the collection of cybersecurity contractual clauses and practices used by Sector Leads and CIIOs • Develop and maintain repository of clauses and sound practices for cybersecurity in vendor contracts

Sector Lead

Role	Champion uptake of the Handbook for CIIOS within its sector, facilitate sharing of sound practices with CSA, Sector Leads and CIIOs
Responsibilities	• Collaborate with other Sector Leads to facilitate information sharing across sectors • Share sound negotiated contractual terms with CSA • Collaborate with international groups and counterparts in other countries to facilitate information sharing on sound practices for including cybersecurity in vendor contracts

CIIO

Role	End user of the Handbook, contribute clauses to the repository and use sound clauses during contract negotiation
Responsibilities	• Share clauses and guidance for including cybersecurity in vendor contracts with Sector Leads and CSA • Access Handbook to refer to sound practice clauses for cybersecurity during contract negotiation with CII vendors • Share sound negotiated contractual terms with CSA

Vendor

Role	Partner with CIIOs and provide technology for CIIs, maintain strong and transparent relationships with CIIOs and maintain security and resiliency of its own organisation and its services or products
Responsibilities	• Develop mutually beneficial relationships with CIIOs that incorporate cybersecurity as a central tenet of the relationship • Strengthen its cybersecurity posture by taking a risk-based approach towards cybersecurity • Maintain security controls and conduct regular assurance activities to ensure continued compliance with security requirements of CIIOs and CSA

Chapter 7:   Vendor Certification Programme

Taking an ecosystem approach to the challenge of cyber supply chain resilience requires incentives to drive practical action by vendors without placing requirements that are too onerous and may end up discouraging them from conducting businesses in Singapore. The Vendor Certification Programme is a scheme for identifying, recognising and establishing a coherent set of cybersecurity standards and certification schemes expected from vendors. Certification is foundational to structure incentives to recognise vendors who have achieved cybersecurity standards and certifications, which can help to raise the baseline cyber hygiene of vendors to meet CIIO cybersecurity requirements. The vendor certification programme can also incentivise vendors who have adopted sound cybersecurity practices to further improve their cyber hygiene or have gone out of their way to achieve cybersecurity standards and certifications. This is a longer-term initiative to improve the overall cybersecurity posture in Singapore.

7.1. The challenge to overcome: vendors are not incentivised to adhere to cybersecurity requirements or improve capabilities for CIIOs

Vendors maintain their cybersecurity capabilities aligned to their organisational, technology and risk approaches. They are limited in using their cybersecurity capabilities and risk posture as a signal for a quality or price premium on their products and services. There are few other incentives for vendors that encourage them for improving their cybersecurity hygiene or meeting the requirements set out by CIIOs. In addition, for a small country with limited bargaining power, CIIOs often do not have strong negotiation power with vendors to adhere to cybersecurity requirements or encourage vendors to improve their cybersecurity capabilities.

While the larger players in the certain market may invest in their cybersecurity capabilities as they see tangible benefits or may even be offering cybersecurity as one of their services, it cannot be assumed across the board, especially in vendors providing services that has little to gain with their investment in cybersecurity than in other aspects of their business where they can see direct and tangible gains.

Within the vendor market, vendor capabilities vary widely between sectors, highlighting the need for incentives to encourage improvement towards a consistent baseline.

7.2. The approach: vendor certification programme to improve vendor's cybersecurity hygiene

The Vendor Certification Programme is a scheme that assesses the applicability, relevance and effectiveness of international, regional, national and industry cybersecurity standards and certification schemes, to develop a repository of certified vendors. The Programme aims to create a framework which increases the value of standards and certification for greater uptake by vendors, as widely recognised standards and certification schemes can be applied to a larger number of markets across borders especially in the context of global cyber supply chain where suppliers offer products and services globally, and many operators have sites in multiple countries and jurisdictions. Combining existing cybersecurity standards and certification schemes into a definitive approach will enable a comprehensive coverage of cybersecurity risks mitigation at various stages of the supply chain. The set of standards and

certification schemes will provide multiple levels through which vendors can progressively improve their cybersecurity maturity.

The Vendor Certification Programme involves an exploratory study to:

1. Identify, assess, evaluate and curate the various existing international and regional standards and certifications related to supply chain cybersecurity. Sector leads are encouraged to augment the effort by including industry-relevant standards and certifications.
2. Select the relevant standards and certifications to be leveraged. The selection approach of the relevant standards will be driven by the cybersecurity threat landscape and the associated cybersecurity risks.
3. Support the onboarding and ongoing development of vendors.

The Programme can be further enhanced with defining a set of baseline cybersecurity controls which can be used to:

- **Provide incentives** to vendors who have established cybersecurity controls to improve their cyber hygiene

- **Boost confidence levels of CIIOs** that vendors have achieved a set of baseline cybersecurity controls to defend against cyberattacks

- **Develop a central whitelist** of standards, certifications and sound practices to help vendors develop their maturity in managing cyber supply chain risks

Beyond the direct incentive of streamlined contracting with CIIOs, a standards and certification scheme offer the secondary effect of nudging the vendor ecosystem towards catalysing a culture of competitiveness with cybersecurity as a key differentiator for vendor products. Vendors could use the standards and certifications as a mark of assurance for their customers, raising the level of trust between vendor and customer. This trust may make it more likely that a customer will choose a vendor over another or that a customer may be willing to pay premium for a product, leading to better business outcomes for the vendor—positioning cybersecurity as a potential avenue for competitive differentiation over other uncertified vendors. In a marketplace of similar vendors, standards and certifications are incentives for differentiation, which could raise the level of cybersecurity in the entire vendor ecosystem. This certification not only benefit major vendor players who may already have appropriate cybersecurity posture, it also helps lesser known and smaller industry players gain trust from current and potential clientele that they are reliable despite their size.

With the evolving threat landscape and emerging technologies, this initiative will be an iterative process and effort to study the applicability of new and existing standards and certification schemes, encouraging its adoption and uplifting vendors towards a more secure cyber supply chain ecosystem.

7.3. The benefits of vendor certification

The Vendor Certification Programme provides clear, actionable benefits to CSA, Sector Leads, CIIOs and vendors, including:

- Defining the baseline cybersecurity requirements as the minimum standard required of CII vendors and improving the overall standard of CII vendor cybersecurity

- Enhancing the baseline cybersecurity requirements of CII vendors to the level required by CIIOs as stipulated in the Cybersecurity Code of Practice (CCoP)

- Uplift cybersecurity requirements of vendors with the incentivisation of streamlined contractual process for vendors through a curated set of standards and certifications

- Increasing the negotiation power of CIIOs to compare the cybersecurity capabilities of vendors and choose certified vendors over uncertified vendors

- Improving competitiveness and increasing business interest for certified vendors

7.4. The role to be played by CII stakeholders

CSA

Role	Champion the Vendor Certification Programme and orchestrate its rollout, collaborate with government agencies and international organisations to extend certification schemes to CII vendors
Responsibilities	• Orchestrate and champion collaboration between sectors and CIIOs to implement the Vendor Certification Programme • Provide cross-sector oversight of Sector Leads to define additional sector specific requirements for certification • Design initiatives that incentivise CII vendors to become certified, uplifting vendor cybersecurity

Sector Lead

Role	Champion the Vendor Certification Programme to CIIOs and vendors within a sector, guide the direction of the certification scheme to consider sector-specific requirements
Responsibilities	• Collaborate with CSA and CIIOs on identifying and defining sector levels requirements • Guide CIIOs in implementing policies, standards, and sound practice • Leverage the CII Cyber Supply Chain Assessment Toolkit to identify vendor cybersecurity and concentration risks specific to the sector • Determine industry-relevant standards and certifications that can promote cyber supply chain health of vendors in their sector

CIIO

Role	Champion the Vendor Certification Programme to vendors, work collectively with CSA, Sector Leads, and vendors to create a mutually beneficial ecosystem that improves cyber supply chain resilience
Responsibilities	• Collaborate with other CIIOs in their industry to manage industry-specific risks and share information • Encourage vendors to undergo certification for a simplified contracting process • Collaborate with vendors to foster ongoing compliance with CSA's cyber supply chain policies and standards

Vendor

Role	Provide technology to CIIs, maintain security and resiliency of its own organisation and services or products to protect CIIs and seek certification to increase business edge
Responsibilities	• Strengthen the organisation's cybersecurity posture by taking a risk-based approach towards cybersecurity • Leverage resources from CSA and apply sound practice principles to have organisation certified under Vendor Certification Programme • Maintain cybersecurity controls and conduct regular cybersecurity assessments and reviews to ensure continued compliance with cybersecurity requirements • Adopt and maintain sound cybersecurity practices and hygiene, in accordance with the requirements of CIIOs and CSA through regular assessments and reviews

Chapter 8:   Cyber Supply Chain Learning Hub

The success of the Programme requires a diverse set of stakeholders from different organisations working together to address a challenging and complex issue through a range of initiatives. Improved CII cyber supply chain resilience requires commitment from senior leaders aligned to a consistent and precise risk management story incorporating business needs and value. To reduce the information asymmetry between CII vendors and CIIOs on cyber supply chain issues, the knowledge, transparency, awareness and appreciation of cyber supply chain risk management topics must shift from a technical domain to a whole-of-organisation concern. Setting up a learning hub for cross-functional knowledge sharing and training resources is important in addressing this.

8.1. The challenge to overcome: limited appreciation of risks from non-technology focused personnel and senior leaders

Across CIIOs, cyber supply chain risk is perceived by procurement and non-technology focused senior leaders to be a technology risk requiring a technology solution. Accountability of cyber supply chain risks is limited outside of technology and cybersecurity teams and isolated from the business resulting in a lack of attention and effort placed on improving resilience.

An extension of this challenge is the resulting limited awareness of cyber supply chain risks, the materiality of potential impact of these risks and the need for action to increase resilience nationally.

8.2. The approach: a learning hub with for cross-functional knowledge sharing and training resources

The Cyber Supply Chain Learning Hub (the 'Hub') is a knowledge sharing platform and provider of ongoing education programmes for cyber supply chain risk management topics for Singapore. The goal is to provide awareness and training resources to cross-functional business, procurement and technology stakeholders from Sector Leads, CIIOs and CII vendors aligned to national regulations and global sound practice.

The Hub is to be delivered as an online knowledge sharing platform for self-service to CII stakeholders. Ongoing education and training programmes will be available. The content is platform agnostic and will be ready to be used in existing industry forums that are relevant to the target audience.

Content for the Hub is curated around the following principles to ensure engagement with the target audience:

- **Accessible.** Content that is easy to understand by stakeholders with different levels of technical cyber knowledge.

- **Audience-centric.** Content that is relevant to the role and scope of work of the audience.

- **Actionable.** Content that provides actionable information and can be easily adopted by the audience to address cyber supply chain risk management challenges.

- **Current.** Content that includes the latest information, relevant to the rapid changes in cyber supply chain risks.

- **Community generated.** Content that includes case studies, intelligence and practices generated from CIIO experiences.

Content modules are split along four broad segments to account for differing objectives of varying stakeholder types:

- **Core.** Knowledge and skills expected from personnel involved in the management of CIIs. Includes compliance requirements for CIIs and general cyber supply chain risk management guidelines.

- **Sector specific.** Knowledge and skills expected to manage cyber supply chain risks in a specific sector. Includes sector specific sound practices, information and intelligence on the latest threats and risks in the sector.

- **Technical.** Knowledge and skills expected of technology and cybersecurity teams involved in managing CIIs. Includes implementation advice on technical cyber supply chain risk management controls.

- **Business.** Knowledge and skills expected of business and procurement stakeholders involved in the vendor management process for CIIs. Includes regulatory requirements on vendor management and guidance on the contractual process.

8.3. The benefits of increased awareness and appreciation

The Learning Hub provides clear actionable benefits to CSA, Sector Leads, CIIOs and vendors, including:

- Enabling improved cyber supply chain risk management of CIIOs through increased knowledge, transparency and awareness of the topic

- Elevating the topic of cyber supply chain resilience from a technology challenge to an organisational imperative for CIIOs, Sector Leads and vendors and facilitating Senior Leadership buy-in for further CII cyber supply chain initiatives

- Reducing the expertise gap between organisations and sectors by increasing the knowledge of procurement teams in CIIOs with limited exposure to cyber supply chain topics

- Streamlining training efforts and reducing cost for CIIOs with a centralised knowledge sharing platform and training resources

- Developing a community of practice for cyber supply chain risk management across Singapore

8.4. The role to be played by CII stakeholders

CSA

Role	Champion the Learning Hub to industries, orchestrate its creation, curate content and develop industry partnerships
Responsibilities	• Develop, source, commission and curate training content to be hosted and disseminated from the Learning Hub • Design training programmes for CII stakeholders • Facilitate partnerships with industry groups to deploy training through existing channels • Advocate the Learning Hub to senior leaders at CIIOs

Sector Lead

Role	Advocate use of the Learning Hub, engage CIIO senior leaders to heighten the appreciation of cyber supply chain risks and facilitate partnerships with industry groups to disseminate the message
Responsibilities	• Engage senior leaders, executives and procurement teams of its sector's CIIOs to build awareness and appreciation of cyber supply chain risks using content and training in the Learning Hub • Facilitate partnerships with industry groups to deploy training to senior leaders through sector specific channels and forums

CIIO

Role	Use the Learning Hub to identify practices to better protect CIIs, engage senior leaders and upskill its organisation towards better cyber supply chain risk management
Responsibilities	• Engage senior leaders, executives and procurement teams in its organisation to build awareness and appreciation of cyber supply chain risks using content and training in the Learning Hub • Develop the skills and improve the practices of CII stakeholders within CIIOs using content and training in the Learning Hub • Contribute sound practices and case studies to CSA to add additional Learning Hub content

Vendor

Role	Use the Learning hub to identify practices to provide greater cybersecurity and resilience to CIIOs, adapt its products and services based on awareness and appreciation of the risks faced by the CIIOS in its sector
Responsibilities	• Participate in training activities and events • Understand the requirements of engaging with CIIOs and providing products or services to CIIs • Understand key cyber supply chain risks in the sector and ways to mitigate them when providing products and services to CIIs

Chapter 9: International Cooperation

The immediate focus of the Programme is to push forward on the foundational activities that improve CII cyber supply chain resilience for essential services in Singapore in response to increased digitalisation and changing threats and risks. However, the globally interconnected nature of cyber supply chains means that over time, individual reactions to cyber supply chain risks from individual countries will no longer be sufficient. Singapore will need to raise its engagement and collaboration with international partners further to collectively address global cyber supply chain challenges

9.1. The challenge to overcome: globally connected supply chains require a globally connected response

The global nature of the cyber supply chain requires international cooperation for cyber supply chain risk management. Countries are approaching the challenge with isolated efforts, attempting to gain visibility into the cyber supply chain risks and threats facing their critical infrastructure to varying degrees of success.

With most technology vendors working on global scale, there is an opportunity to combine efforts between countries to improve the visibility of the cyber supply chain and push for improved cybersecurity and resilience requirements. Large technology vendors have significant market power, making it difficult for CIIOs in individual countries to negotiate cybersecurity requirements on baseline security practices.

Additionally, cyber supply chain incidents like SolarWinds are occurring on a global scale and affecting governments and organisations in many countries. CIIOs are facing challenges in understanding if they have been affected by cyber supply chain incidents in a timely manner and being able to limit the blast radius and mitigate the impact quickly when affected. Improved global visibility of the shared cyber supply chain has the potential to improve this for CIIOs.

International cooperation can also generate momentum to improve the cybersecurity capabilities of vendors that are common across multiple countries. Standardising the cybersecurity requirements for vendors from multiple countries can improve the bargaining power of purchasers to enforce the requirements.

9.2. The approach: collaboration and cooperation

International cooperation to improve the resilience of the global cyber supply chain involves developing collaboration mechanisms for cyber supply chain risk management with international partners and strengthening global cyber supply chain visibility and information and intelligence sharing for improved coordination and response activities.

The international partners considered for this initiative include:

- Governments
- Country groups
- Industry groups and non-government organisations
- Procurers of digital technology services (e.g., multiple international organisations that subscribe to the same cloud service providers)
- Large and/or critical vendors (e.g., vendors of linchpin technologies such as OT and digital services (i.e., railway technology, cloud, large payment systems))

This initiative focuses on four collaboration mechanisms to instil and strengthen international cooperation for improved cyber supply chain resilience:

- **Regular dialogue**

  Identify existing forums and develop new forums and platforms for information and intelligence sharing for cyber supply chain risk management. Improve visibility of global cyber supply chains and improve transparency into global risks, while communicating global trends and best practices for risk mitigation including country level cyber supply chain management methodologies and country level cyber supply chain incident response processes.

- **Capacity-building**

  Enhance global cybersecurity capacity-building to collectively mitigate or respond to cyber supply chain risks adequately and effectively through regional and international coordination. This could include collaborative incident detection, reporting and coordinated response activities.

- **Policy intervention**

  Contribute to the development and promotion of interoperable regional and international cybersecurity standards for vendors and consistent policy approaches of contributing countries to cyber supply chain risk management.

- **Mutual recognition of norms and standards**

  Establish mutual recognition of norms and standards for cyber supply chain risk management (e.g., disclosure agreements for incident reporting between vendors and likeminded groups of countries, recognising the Vendor Certification Programme by other countries)

9.3. The benefits of international cooperation

International cooperation provides sustainable long-term benefits to Singapore and regional and international partners, including:

- Strengthening Singapore's position in improving the cybersecurity and resiliency of the global cyber supply chain and increasing the negotiation leverage for countries banding together to request for higher baseline cybersecurity capabilities of global vendors

- Increasing efficiency of responses to global cyber supply chain incidents through timely information and intelligence sharing and coordinated cross-border responses

- Aligning standards for baseline cybersecurity and resiliency requirements of vendors with international counterparts, driving a consistent global approach to risk management

- Encouraging regional and international collaboration to improve transparency in continuous risk management for CIIs at a global level

- Empowering CIIs with a better slate of tools and information to respond and react to cyber supply chain risks

9.4. The role to be played by CII stakeholders

CSA

Role	Facilitate and advocate for bilateral, regional and international cooperation and cyber supply chain capacity-building on behalf of Singapore
Responsibilities	• Identify and participate in forums and platforms for regional and international engagement and cooperation • Coordinate Singapore's contribution to collective capacity-building

Conclusion and Next Steps

Strengthening the cybersecurity and resilience of Singapore's CIIs to preserve and enable essential services is a significant priority for Singapore. Pivotal to this effort is managing the risks that arise in the extended cyber supply chain.

The CII Supply Chain Programme is a blueprint for CSA, Sector Leads, CIIOs and vendors to build cybersecurity and resilience into the CII supply chain in response to an ever-evolving threat landscape and increased digitalisation. The Programme is the beginning of a journey towards a secure and resilient future for Singapore's CIIs.

The initial focus of this important journey is to achieve increased visibility of the national CII cyber supply chain. The initial step is developing and deploying the CII Cyber Supply Chain Assessment Toolkit, a foundational item, to all CIIOs to collect a baseline inventory of all Tier 1 CII vendors. From this, there can be immediate action to manage national risks at a national level, with the evolution towards nth Tier visibility when Tier 1 data are ingested into an advanced data model.

The next focus is to capitalise on the Programme's momentum by deploying the Cyber Contractual Handbook to improve the collective power of CIIOs to collaborate and negotiate for improved cybersecurity requirements with CII vendors. As a follow-on activity, the Vendor Certification Programme furthers the cybersecurity requirements for vendors and shapes incentives for vendors to improve their capabilities. These initiatives cover the buy and sell sides of the CII market and can work synergistically to improve the cybersecurity and resilience of both vendors and CIIOs.

Finally, take steps towards developing national awareness and appreciation of cyber supply chain topics to improve the likelihood of success and uptake of the Programme. Implement the Cyber Supply Chain Learning Hub and disseminate content and training to senior leaders and procurement functions at CIIOs to elevate the topic of cyber supply chain resilience to an organisational imperative. Efforts in cyber supply chain education can be built on to encourage buy-in from CIIOs for other Programme initiatives.

Cybersecurity and resilience in the supply chain is a collective responsibility. Success of the Programme requires a multi-stakeholder effort with active contribution to the implementation and operation of the initiatives across the national, sectoral and organisational levels. Longer term, Singapore can reach outwards to contribute its learnings internationally and contribute to building a secure and resilient international cyber supply chain.

Acknowledgements

Programme Sponsor

Lim Thian Chin, Director (CII), Cyber Security Agency of Singapore

Contributors

Cyber Security Agency of Singapore

Christopher Anthony, Deputy Director

Tracy Thng, Senior Consultant

Sean Lai, Consultant

Ang Kar Min, Consultant

Boston Consulting Group

Michael Tan, Managing Director and Partner

Paul O'Rourke, Managing Director and Partner

Michael Meyer, Managing Director and Partner

Alain Schneuwly, Managing Director

Nadya Bartol, Managing Director

Miri Marciano, Associate Director

Colin Teo, Principal

Sugar Chan, Manager

Yuan Shuai, Senior Consultant

Luke Flanagan, Senior Consultant

Jeffrey Ng, Senior Consultant

Wong Jia Ping, Consultant

Our sincere thanks to the organisations and individuals who have contributed to the development of the Programme:

Changi Airport Group

Citibank Singapore Ltd.

Civil Aviation Authority of Singapore

Cybersecurity Agency of Singapore

Daniel Cheng, Senior Manager (Cybersecurity), Civil Aviation Authority of Singapore

DBS Bank Ltd.

Energy Market Authority

Government Technology Agency

Home Team Science and Technology Agency (HTX)

Infocomm Media Development Authority

Integrated Health Information Systems (iHiS) Pte. Ltd.

International Organization for Standardization

Land Transport Authority

M1 Ltd.

Maritime and Port Authority of Singapore

Mediacorp Pte. Ltd.

Ministry of Defence

Ministry of Health of Singapore

Ministry of Home Affairs

Monetary Authority of Singapore

National Institute of Standards and Technology

PSA International Pte. Ltd.

Public Utilities Board

S. Rajaratnam School of International Studies

SBS Transit Ltd.

Singapore LNG Corporation Pte Ltd.

SMRT Corporation Ltd.

SP Group Pte. Ltd.

Toh Kai Seng, Senior Manager (Cybersecurity – Global Governance), PSA International Pte. Ltd.

YTL Corporation Berhad

References

[1] Microsoft and IDC, "Culture of Innovation: Foundation for Business Resilience and Economic Recovery in Asia Pacific"

[2] Statista, "Internet of Things - number of connected devices worldwide 2015-2025", https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] Cybersecurity Ventures, "Annual Cybercrime Report 2020", https://cybersecurityventures.com/annual-cybercrime-report-2020/

[4] The *New York Times*, "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers", https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html

[5] *WIRED Magazine*, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[6] UK National Audit Office, "Investigation: WannaCry cyber-attack and the NHS", https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[7] VMWare Carbon Black, "Global Incident Response Threat Report 2020", https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-global-incident-response-threat-report-the-cybersecurity-tipping-point.pdf

[8] The Conversation, "What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake", https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

[9] *The Guardian*, "What you need to know about the biggest hack of the US government in years", https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department

[10] *The New York Times*, "Hundreds of Businesses, From Sweden to U.S, Affected by Cyberattack", https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html

[11] ENISA, "ENISA Threat Landscape 2021", https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Technical Appendix A: Vendor Management Methodology

Third-party vendors are an integral part of today's business landscape. Appropriate supply chain cyber risk management is essential to manage and monitor any risks from third-party vendors or technology vendors. The recommendations outlined below involve a multi-step process to assess, monitor, and manage potential vendor cyber risk to maintain the cybersecurity and resilience of CIIs. CIIOs will have access to the CII Cyber Supply Chain Assessment Toolkit to track and analyse the data generated from this process.

1. Process for managing vendors

A robust initial assessment should be undertaken to directly address any cybersecurity risks before the onset of a formal contractual relationship. The organisation should also proceed with ongoing assessment activities with existing vendors, and ensure new vendors are appropriately onboarded to maintain oversight of the entire supply chain lifecycle and manage cyber supply chain risks across all vendors.

1.1 Procurement and intake

Organisations should employ a comprehensive assessment process at the point of engagement. This provides a process to identify any early risks and ensure appropriate mitigation measures are put in place.

1. **Vendor cybersecurity assessment.** Undertake a vendor cybersecurity assessment prior to intake, ensuring the vendor has the appropriate prerequisite cybersecurity controls in place prior to entering into a contract.

2. **Vendor contracting.** Mandate the minimum cybersecurity controls and obligations that a vendor must adopt throughout the business relationship. This should be clearly stated and agreed to in official contract documents.

3. **Inventory and baseline risk assessment.** Add vendors, and vendors of vendors where relevant, to a centralised vendor inventory which should detail the cyber risks of each vendor and provide a view of overall cyber supply chain risk in the organisation.

1.2 Ongoing risk management

Cybersecurity threats continue to evolve, necessitating ongoing management and engagement with vendors to mitigate risks. A robust evaluation process should be undertaken periodically to identify new risks or weaknesses which may exist in the vendor ecosystem.

1. **Gap remediation.** Collaborate with vendors throughout a relationship to address any identified cybersecurity gaps, starting with those deemed to have the highest cyber supply chain risk level.

2. **Resiliency planning.** Include most important vendors in business continuity and disaster recovery plans and exercises to ensure end-to-end resilience.

3. **Periodic reassessments.** Conduct regular assessments using questionnaires, alongside technical testing, to record any pertinent changes in a vendor relationship (e.g., changes to sharing of sensitive data). Ensure the vendor continues to adhere to minimum cybersecurity requirements.

4. **Training and support.** Develop training, guidance and support for vendors, providing an organisation-wide understanding on key risks associated with working the organisation, and ensuring appropriate standardisation of onboarding and assessment for new vendors.

5. **Information sharing.** Share relevant information with regulatory bodies and industry peers to inform sound practice and maintain a secure ecosystem.

6. **Incident response.** Collaborate with vendors to prepare for a cybersecurity incident, and ensure that key contacts, procedures, and processes are established and understood to enable a rapid response to any future real-world incident.

7. **Vulnerability management.** Establish a system for vendors to communicate quickly and clearly with customers if any vulnerabilities are identified.

8. **Programme tracking.** Develop appropriate metrics to track and report on cyber supply chain operations.

1.3 Organisational procurement process

A standardised vendor procurement process with clear assessment and onboarding procedures should be established by each CIIO. This will help ensure that cybersecurity standards are maintained across the vendor ecosystem and reusable for further vendors.

1. **Centralised intake.** Develop centralised vendor intake/onboarding processes across the organisation, ensuring all vendors are included in a well-maintained vendor inventory.

2. **Evaluation.** Establish standard vendor evaluation criteria to include cyber supply chain considerations such as vendor cybersecurity posture, resiliency, and continued compliance with any applicable cyber and privacy regulations.

3. **Contracting.** Establish a boilerplate contract language to cover all cyber supply chain considerations, ensuring faster onboarding without compromising on cybersecurity. This should include metrics and service-level agreements that incorporate incident notification timeframes and procedures, minimum cybersecurity expectations, understanding of periodic cybersecurity reviews, and testing to be performed on a vendor.

2. Process for tracking vendors and performing risk analysis

2.1 Vendor identification

All vendors should be identified to understand where both new and existing vendors sit within, and interact with, the CII framework.

- **Vendor identification and mapping.** Identify the list of CII assets and other related assets within the perimeter boundaries of CIIs, as defined by each CIIO within the relevant area of operations. Map all in-scope vendors against the organisation's

ecosystem of products and services to provide an overview of each entity's positioning and relevance in the overall supply chain.

- **Vendor assessment.** Pinpoint which vendors are material to the continued operation of CII assets. Vendors within the scope of this Programme are defined as any vendors that directly provide products or services to the components within the perimeter of CIIs. Details of this scope are outlined in Chapter 3, and the types of vendor assessments to be performed are described in the following two sections.

2.2 Vendor importance assessment

Understanding the importance of individual vendors to the continuation of overall operations of an organisation is a key part of supply chain risk management. Each vendor should be assessed and stratified by CIIOs based on key attributes such as:

- **Dependency on vendor.** Measure the degree to which the organisation depends on a given vendor for business continuity, as well as the organisational and financial damage which could be inflicted if a vendor experiences prolonged recovery times from an adverse incident.

- **Degree of impact.** Measure the impact (e.g., financial, operational, etc.) that a compromise of the vendor would have on the CIIO's ability to deliver essential services.

- **Degree of access.** Measure the level of access that a vendor has to the organisation's IT networks, including remote access, as well as access to sensitive data and physical facilities. In addition, measure the level of access or control CIIO has on relevant vendor systems related to the operation of CII assets.

Further iterations of the vendor importance assessment may consider the location of the vendor in the end-to-end supply chain, and how that links to overall ecosystem continuity and resilience.

2.3 Vendor maturity assessment

A baseline cybersecurity assessment of the vendor should be conducted, combining self-reported data points, such as those from a questionnaire, with external expert validation such as external vulnerability scans or cybersecurity penetration testing exercises. This should inform an overall risk score to categorise the vendor based on identified weaknesses and strengths. Such risk assessment should be categorised according to several key cybersecurity domains:

- **Cybersecurity programme.** Existence and suitability of internal cybersecurity procedures and processes. This should include all recognised cybersecurity certifications the vendor has received, and regulations the vendor has complied with.

- **Incident response and resiliency.** Availability of clear incident response plan to prepare, detect and analyse, contain and recover, and align on appropriate activities during and after an incident.

- **Secure development.** Timeline and framework for designing, developing, and testing custom code/software, from inception to final decommissioning.

- **Third-party management.** Risk management framework to tackle third-party risks from vendors.

- **Network security.** Level of protection applied to the organisation's networks.

- **Logging and monitoring.** Standard procedures to log and monitor all adverse events and cybersecurity risks, with defined logging requirements and goals.

- **Data protection.** Processes to maintain the security, confidentiality, and integrity of data as part of a clearly defined data management process.

- **Vulnerability management.** Established procedures to identify and manage vulnerabilities.

- **Identity and access management.** Identity, authentication, and authorisation controls to limit access to sensitive resources.

2.4 Vendor risk assessment

All vendors should be assigned a risk score based on importance and maturity assessments, conducted according to the process outlined in Steps 2.2 and 2.3 of this process.

- **Determine gaps.** All gaps between the current state of vendor operations and defined cybersecurity requirements should be identified.

- **Work to address gaps.** Work with vendors with identified gaps to support them to improve resilience and bridge those gaps.

3. Ongoing activities

Processes to manage communication and incident reporting across the ongoing partnership are vital. This framework should cover the full lifecycle of data, technology, and partnership from inception to offboarding.

- **Vendor vulnerability management and incident response.** Establish clear channels of communication based on contractually agreed upon terms to ensure rapid response in the event of a cybersecurity incident and provide the ability to quickly mitigate risks and apply patches to impacted systems.

- **Contract renegotiation.** For existing contracts, work with vendors to revise contract to include new vendor cybersecurity requirements.

- **Vendor end-of-life and offboarding.** Work with vendors to securely dispose assets, data, and other potential end-of-life cybersecurity risks. Ensure decommissioned assets are replaced with suitable alternatives as necessary to ensure no ongoing vulnerabilities or gaps.