UNIVERSITY OF TWENTE.

A Thesis
submitted for the fulfilment of the requirements for the degree of
Master of Science (M. Sc.)
in
Business Information Technology
Presented to the
Faculty of Electrical Engineering, Mathematics and Computer Science

Cyber Supply Chain Risk Management in the Netherlands:
Investigating Structural Elements and Drivers in the Context of EU-Cybersecurity Regulation

By
*J*onathan Weiss
Master of Business Information Technology (M. Sc.)
Electrical Engineering, Mathematics and Computer Science

Graduation Committee:
*d*r. A. Abhishta | Senior Examiner
Behavioral, Management and Social Sciences

*d*r. ing. F.W. Hahn | Examiner
Electrical Engineering, Mathematics and Computer Science

M. Sc. J. Visser | Advisory Member
Senior Manager, PwC Netherlands

Enschede, the Netherlands, August 18, 2023.

Acknowledgements

This thesis is created in collaboration with the
business unit for Cybersecurity, Forensics & Privacy of
PwC Netherlands.

I would like to express my deepest appreciation to
Jan Visser,
Suzie Bernards,
Bram van Tiel,
Jaap Halfweeg
and all other colleagues for supporting me throughout the process of writing this thesis.
A special thanks to all interview participants for their time and valuable contribution.

About PwC: PwC Netherlands' Cybersecurity, Forensics, and Privacy unit offers comprehensive solutions for businesses navigating the digital landscape. It assists organisations in crafting an effective cybersecurity strategy that ensures compliance with regulatory standards and governance. The unit also provides services for threat, incident, and crisis management, helping firms bolster their response to potential attacks. Furthermore, PwC helps businesses adhere to evolving privacy laws and regulations, supporting them in setting up robust privacy programmes. The unit also aids in information protection and cloud security, helping businesses maintain control over data in an increasingly complex digital environment. Additionally, PwC implements effective Identity and Access Management processes and technology, considering user experience, compliance, and threat mitigation. The team offers resilience services against ransomware and red, blue, and purple teaming for proactive security checks, enhancing an organisation's preparedness against cyber threats. Find more information here.

Abstract

Purpose: *The growing complexity of supply chain (SC) ecosystems, along with the proliferation of high-profile SC attacks has forced organisations to gain visibility and control over the corresponding risks. The worsening consequences of such attacks have brought the attention to board level, prioritising SC cybersecurity. This thesis aims to explore Cyber Supply Chain Risk Management (C-SCRM) within organisations in the Netherlands as a possible approach to overview the complex risk landscape. Subsequently, the requirements of current and upcoming EU cyber regulations are taken into account. Additionally, this work aims to contribute to the establishment of a shared paradigm within the field of research and align used terminology. The thesis takes up a holistic organisational perspective and investigates concepts that support the successful implementation and operation of C-SCRM.*

Methods: *This exploratory study uses grounded theory within a qualitative inductive approach. A concept-centric systematic literature review is carried out for initial data gathering. The data is subsequently used for a conceptual framework analysis. Ten semi-structured interviews are then used to specify the conceptual framework and explore the concepts in practice. The interviews are analysed using a three-step grounded analysis consisting of open, axial, and selective coding. The results are then used to synthesise theory and practice.*

Findings: *The findings confirm the growing complexities and risks associated with modern (cyber) SCs. They illustrate the pressing need for organisations to address these issues due to the evolving regulatory landscape in the EU. Theoretical research is limited and often involves the use of unaligned terminologies and definitions. By studying the organisational perspective of C-SCRM, this thesis uncovers structural elements, drivers and main outcomes for successful implementation and operation of C-SCRM. The corresponding interviews indicate that while organisations show increasing awareness and willingness to implement robust C-SCRM practices, the implementation lags behind. It remains very complicated and costly for organisations to determine the right approach and most organisations lack the needed prerequisites to avoid additional efforts. Investigating the perception of the identified concepts of the conceptual framework in practice reveals the state of implementation within organisations in the Netherlands and highlights current best practices. This study provides sound recommendations for organisations to act immediately, under consideration of regulatory requirements.*

Conclusions: *Despite the rising awareness, organisations in the Netherlands currently cannot keep up with the rapid pace set by threat actors. Upcoming EU regulation is deemed to advance current initiatives and drive standardisation. The identified structural elements and drivers presented in this thesis may enable organisations to increase the speed of their progress. A collaboration between policymakers, research, industry consortia and important market players is needed to tackle the challenge in an effective way.*

Keywords: *supply chain cybersecuriy, cyber supply chain risk management, c-scrm, cyber regulation, NIS2, CRA*

Contents

List of Figures

List of Tables

List of Acronyms

AICPA American Institute of Certified Public Accountants. 26, 40, 55

BIO Baseline Informatiebeveiliging Overheid. 8, 40

C-SCRM Cyber Supply Chain Risk Management. 1, 2, 5, 6, 8–12, 15, 17, 21–31, 36–38, 40–49, 51–63, II–V

CRA Cyber Resilience Act. 1, 7, 8, 46, 56, 63

CSC Cyber Supply Chain. 2, 3, 5, 6, 14–22, 25–27, 30, 36, 37, 41, 52–55, 59, 60, 62, III, V

ENISA European Union Agency for Cybersecurity. 6, 14, 59

ICT information and communications technology. 1–3, 6, 7, 16, 17, 19, 21, 25, 27, 32, 54, 57, 59, 62

NIS2 Network and Information Security Directive. 1, 7, 8, 46, 56, 62, 63

NIST National Institute of Standards and Technology. 6, 14, 17, 21

SC supply chain. 1–8, 10–12, 16–30, 32, 36–44, 46–64, II, V

SME small and medium-sized enterprises. 24, 27, 30, 60

WEF World Economic Forum. 54, 56

1 | Introduction

> *"The rise of supply chain threats and escalating ransomware attacks are the most pressing cyber challenges the international community needs to address. Business leaders must consider cybersecurity as a risk management issue and balance the trade-offs between security, usability and cost at the Board or C-suite level."*
>
> David Koh, Chief Executive, Cyber Security Agency (CSA), Singapore (2022, p. 8)

In the globalised world supply chains (SC) have become the backbone of the evolving technological ecosystem (Ghadge et al., 2020). Every organisation relies on acquiring information and communications technology (ICT) products and services throughout complex, multi-tier supply chains (Boyens et al., 2021; Nygård & Katsikas, 2022). The results are entangled dependencies and a growing attack surface, potentially being exploited by global threat actors. Over the course of the last three years, they have gained traction, alarmingly fast. SC attacks are continuously increasing over the past few years. The attacks target smaller companies with a weaker cybersecurity posture in the SC to propagate towards their main target (Creazza et al., 2022).

Recent surveys confirm that between 39% and 62% of organisations were already affected by third-party cyber incidents, and 46% already experienced an incident due to a software SC attack (Papaphilippou et al., 2023; Pipikaite, 2022; Splunk Inc., 2023). In practice, attacks can originate both, from partners upstream and downstream in the SC with severe consequences, even if robust cybersecurity measures are in place (Colicchia et al., 2019). Without a major paradigm shift the worldwide economic damage of software SC attacks alone is estimated to reach over $80 billion by 2026, which is an increase of 76% (Juniper Research Ltd., 2023). The negative impacts have created an urgent need for organisations to gain visibility and control over these complex ecosystems and corresponding threats (Boyson et al., 2022). The rising number of SC cyber attacks underscores that reliance on technical security solutions, simply put as just "firewalling", is inadequate and strategically insufficient in protecting an organisation from falling victim to a SC cyber attack (Pandey et al., 2020; Shankles et al., 2013). Thus, organisations must adopt a comprehensive approach that goes beyond technical measures and embraces the interconnectedness of the SC to effectively address cyber risks (Colicchia et al., 2019). Yet, resilience in the Netherlands has not reached the required level (NCTV, 2023).

The topic has experienced significant momentum following the release and announcement of the EU's latest Network and Information Security Directive (NIS2) and the proposal of the Cyber Resilience Act (CRA), requiring organisations to act on their SC cybersecurity. Yet, guidance on how to facilitate this effectively is missing.

Cyber Supply Chain Risk Management (C-SCRM) provides a possible solution to tackle SC cyber risks. However, coordinated and integrated risk management within and between the different levels of organisations, sectors and the national level is still in its infancy, lacking comprehensive studies and a theoretical foundation (NCTV, 2023; Cheung et al., 2021; Topping et al., 2021; Melnyk et al., 2022; Guerra & Estay,

2019). PwC (2023a) Global Digital Trust Insights finds that more than half of worldwide C-level risk and operation officers have serious concerns about their ability to withstand SC attacks. In the realm of cyber attacks, there are no rules, policies, or norms and no organisation, government or individual is immune while the threat is predicted to keep growing in the next years (PwC, 2023b). Thus, collaborative action is needed to guide organisations.

This thesis aims to shed light on the current state of C-SCRM in the Netherlands and will explore structural elements and drivers to develop and operate a holistic C-SCRM. In the subsequent sections of this introduction chapter we elaborate on the study's background in Section 1.1, present the research questions and subsequent research design in Sections 1.2 and 1.3 respectively, and offer an overview of the study's scope in Section 1.4. The structure of this thesis is outlined in Section 1.5.

1.1 Background

In the background of this thesis we first delve into the complexities of current SC ecosystems and afterwards, provide examples of prominent and recent SC attacks. After, we shortly introduce C-SCRM and highlight the influence and interplay of current and upcoming regulations.

1.1.1 Complexity in Supply Chain Ecosystems

To keep up with external performance expectations regarding speed and reliability SCs must be fast, accurate, and agile (Sobb et al., 2020). This has been achieved through the use of various technologies. Sourcing technology solutions of competing vendors in a SC offers various advantages such as low cost, interoperability, rapid innovation, and product feature variety (Boyens et al., 2022). In comparison to traditional SCs, operations nowadays have changed through the increased integration of ICT systems, forming extended information ecosystems (Pandey et al., 2020). Especially the emergence of Industry 4.0 technologies e.g. the Internet of Things, virtual reality, artificial intelligence, and blockchain expand the relationships between SC partners (Ghadge et al., 2020). This has brought up the term Cyber Supply Chain (CSC), easily described as all ICT components of an organisation involved in the value creation and with dependencies to third parties. According to Ludvigsen et al. (2022), modern SCs are mainly characterised by excessive market monopolies, increased network effects and the associated complexity from inter-dependencies as well as a lack of alternatives and transparency. A SC typically includes multiple tiers of suppliers, which in its most complex form is also named the *"ultimate SC"*, and organisations usually only have visibility in first- and second-tier suppliers (Windelberg, 2016; van den Brink et al., 2021). Figure I shows that the upstream complexity can be divided into the number of suppliers in each tier (horizontal complexity), the number of tiers (vertical complexity), and the distribution of the members of a network e.g. geographically (spatial complexity) (Bode & Wagner, 2015). Further, the technological development of the (Industrial) Internet of Things and cyber-physical systems as hybrid systems has eliminated the traditional "air gap" that once separated IT and OT networks. In addition, the increased lifespan of OT devices compared to IT systems (typically 20 to 30 years) has contributed to the emergence of new advanced persistent threats (Nygård & Katsikas, 2022; Cheung et al., 2021).

In summary, the following developments are further raising the importance to understand risks along the CSC:

- The integration of digital assets (information, information technology, new technologies) to enhance the physical infrastructure of SCs.
- The Increased interconnectedness of physical and digital assets and their interaction with cyberspace.
- The complexity of ICT product SCs.
- The destructiveness of cyberattacks with the ability to disrupt a whole SC.
  (van den Brink et al., 2021; Garvey, Samuel, & Kretinin, 2021)

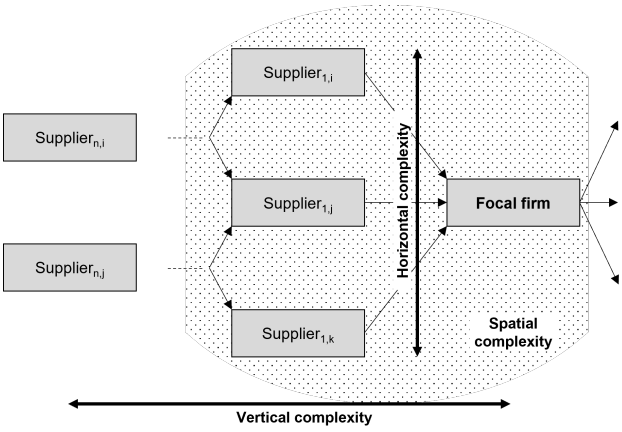

FIGURE I. Horizontal, vertical, and spatial complexity of the upstream SC.
Own illustration, adapted from Bode and Wagner (2015).

The mentioned developments significantly increase the complexity, leading to organisations not having full control and visibility into their SC ecosystems of products they produce or services they deliver (Boyens et al., 2021). It's not enough to only consider the SC of one's own organisation, sector, or country. As sectors and service providers engage in more partnerships, the risk exposure also increases. Often, vulnerabilities and dependencies aren't apparent until an incident occurs. A single incident can reveal that many organisations within a sector rely on a single party. (NCTV, 2023) As a result, these highly interrelated ecosystems significantly broaden the attack surface, with new vulnerabilities and risks that are becoming greater and farther reaching beyond the border of a single company, potentially leading to large-scale national or cross-border impacts. (Schauer et al., 2019; Pandey et al., 2020; Boyson, 2014; NCTV, 2023). However, identifying these risks presents a challenge for organisations due to the information asymmetry between acquirers and suppliers in terms of understanding the underlying structures, which is further amplified by a general lack of trust between partners (Boyens et al., 2022; Pandey et al., 2020). The international dimension, diversity of suppliers, and lack of clear responsibilities further increase the difficulty to manage these risks (Topping et al., 2021). Subsequently, it raises the question if these risks require a different approach than conventional risk management processes (van den Brink et al., 2021).

Recent research highlights the fact that traditional information risk management and current efforts on how to deal with CSC risks are generally focused within the boundaries of the focal organisation and mainly related to reactive technical, and IT-related measures (Colicchia et al., 2019; Ghadge et al., 2020; Creazza et al., 2022; Gani et al., 2023; Melnyk et al., 2022). Colicchia et al. (2019) also find that decision-making is mainly done exclusively by the IT department in isolation from other departments or SC partners. Established standards (e.g. ISO270XX) are mainly driving intra-organisational measures to manage individual risks, without the guarantee that the SC will follow, and thus fails to tackle the overarching issue of the "weakest link" (Ghadge

et al., 2020; Schauer et al., 2019). Although organisations are aware of critical supplier dependencies, they struggle to fully understand the underlying factors (van den Brink et al., 2021). Therefore the literature is unanimous that a coordinated, fully integrated strategic approach beyond the dyad, creating a relationship dimension between people, process, and technology is essential to deal with cyber risks in the SC (Creazza et al., 2022; Gani et al., 2023).

1.1.2 Supply Chain Attacks

In the previous sections, the growing threat of SC compromises and dedicated attacks were highlighted. Therefore, the following will showcase some of the most prominent as well as recent SC attacks and their consequences.

This study will examine SC attacks based on the definition provided by ENISA (2021), which categorises SC attacks as a combination of at least two attacks. Thus, the attacker initiates the first attack to compromise the supplier's assets and subsequently utilises this access to target the customers of other suppliers through a subsequent attack. A more elaborate description of the commonly used attack methods as well as points of penetration is provided in Section 2.4.

Target - 2013

The massive data breach of the retailer Target in 2013 shows that SC attacks are not an entirely new phenomenon. A detailed kill chain analysis of the US Senate (2014) describes the procedure. In this case, attackers managed to install malware on the retailers' point of sale systems that led to the successful theft of the personal information of 70 million customers as well as information from 40 million credit and debit cards. The malware enabled the attackers to collect the information before encryption as plain text data. Anonymous investigators found out that the first malware was already installed two months before Target officially disclosed the data breach. The initial access to Target's systems was gained two months before by stealing the credentials of a heating, ventilation and air conditioning supplier that had remote access to the network through phishing emails. As a consequence of the data breach, Target had to pay a $18.5 million settlement to different states. However, the total cost doesn't stop there. The total cost is estimated at $200 million with a temporary decrease of 46% in earnings (Jones, 2021).

SolarWinds - 2020

One of the most prominent SC attacks affected the software provider SolarWinds in 2020. Attackers gained initial access to their networks through spoofing of the identity and authentication mechanisms of access accounts. After a period of extended information gathering, malicious code was inserted into the source code of the network management system product "Orion". The code was signed and distributed as a part of the update process, infecting more than 18.000 customers and 40 public entities throughout the whole world, including the critical infrastructure with malware (Martínez & Durán, 2021). The consequences included, inter alia, fallout and investigation costs of $18 million and a $26 million settlement over a shareholder lawsuit (Satter, 2021; Kovacs, 2021). Additionally, BitSight estimated that the insured losses incurred by affected organisations for incident response and forensic services efforts amounted to approximately $90 million (Shah, 2021).

US & China - Hardware Tampering

Hardware SC attacks are more difficult to pull off, however harder to detect and potentially more devastating. Thus it is also more difficult to find public examples here. The following briefly describes two examples of proven hardware manipulation. Note, that both scenarios were denied by the accused governments as well as victim organisations. In 2015, during an evaluation of a possible acquisition by Amazon, investigators found tiny malicious microchips, only as big as a grain of rice on the servers' motherboards of the supplier Super Micro Computer. Investigations revealed those chips enabled attackers to access any network associated with the server. The chips had been inserted by a manufacturing sub-contractor in China. Next to Amazon, the chips were found in almost 30 affected companies, including a major bank, government contractors and Apple, who had planned to order more than 30,000 of those servers. (Robertson & Riley, 2018) The US government has long accused Chinese companies, such as Huawei and ZTE, of creating routers and internet devices with backdoor surveillance functionality, allowing the Chinese government to spy on users. Contrary in 2010, NSA documents reveal similar practices within the US. An NSA report disclosed that the agency intercepts US-made routers and servers, installs surveillance tools, and then sends them to international customers. This suggests that warnings against Chinese devices may have also been motivated by the desire to prevent competition with American-made devices, potentially limiting the NSA's surveillance reach. (Greenwald, 2014)

3CX - 2023

A more recent example from March 2023 involves the international voice-over-IP provider 3CX. This incident stood out as a unique case, being the first instance where evidence emerged supporting the cascading nature of a SC attack, where one attack leads to another. The initial analysis revealed that the threat actors first managed to insert backdoor code into a software application of the firm Trading Technologies, which was later installed on the computer of a 3CX employee. This allowed the attackers to spread through the network of 3CX, ultimately infecting a software development server and hijacking a 3CX installer application which infected a large number of their 600,000 customers. Ongoing investigations revealed that the attacker's goal was aimed at cryptocurrency theft. (Greenberg, 2023) The victims of the attack include multiple critical infrastructure organisations in the energy sector from the US and Europe as well as from the financial sector. As the attack is still under investigation up to this day, the precise origin, as well as the consequences, are not known yet. (Vigliarolo, 2023)

The presented examples underscore the severity and complexity of SC attacks, requiring months of dedicated investigation for reconstruction. Especially the examples of hardware manipulation highlight the political involvement on an international scale.

1.1.3 Cyber Supply Chain Risk Management

The concept of the **CSC** is not new. Some authors (Creazza et al. (2022); Garvey et al. (2021); Colicchia et al. (2019)) date the first emergence in the field back to Warren and Hutchinson (2000), who for the first time acknowledged the existence of the **CSC** and corresponding risks. However, the beginning of dedicated research around **C-SCRM** can be dated back to the year 2008, more precisely after the release of the *Comprehensive National Cybersecurity Initiative* by the Obama administration, which admitted the significance of cybersecurity as one of the major challenges of the nation (Bartol, 2014; Boyens et al., 2021).

This is when the National Institute of Standards and Technology (NIST) started to work on publications around guidance on **CSC** risks for federal information systems, later labelled as **C-SCRM** (Boyens, Paulsen, Bartol, Shankles, & Moorthy, 2012). Other early efforts were provided by the NDIA (2008) and SAFECode (Simpson et al., 2009, 2010; Bartol, 2014). Therefore, the discipline has its origin in the secure acquisition of federal IT-Systems in the United States.

In general, the field has seen a broadening of scope over time. Starting with a focus on ICT product SCs (mainly for procurement), **C-SCRM** now aims to cover all cybersecurity-related risks along the end-to-end SC in a continuously adaptive manner, by combining enterprise risk management, SC management, and information security (Boyens et al., 2021; Creazza et al., 2022; Boyson, 2014). **C-SCRM** is classified as an organisational strategy and programmatic activities that constitute an enterprise-wide systematic process for managing the exposure to cybersecurity risks along the **CSC** throughout the development of strategies, policies, and processes (Boyson, 2014; Boyens et al., 2022). Activities include the entire system development lifecycle, including research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, disposal, and overall management of products and services within an organisation (Boyens et al., 2022). Most importantly, **C-SCRM** aims to go beyond technical risks and includes relational factors that impact the coordination among SC partners, ultimately aiming for a high level of integration, that addresses the limitation of focusing solely on individual points in the SC interface (Hampton et al., 2021; Creazza et al., 2022). These two dimensions were earlier also described as a defence in depth (entire system development lifecycle), and a defence in breadth (beyond the focal firm) (Boyson, 2014). As such, adopting a management perspective that incorporates a blend of technical and organisational practices is essential when approaching **C-SCRM** (Gani et al., 2023).

Although **C-SCRM** has existed for some time, research is limited (Nygård & Katsikas, 2022). This could be due to the versatility of the individual concepts and thus the lack of prioritisation in the holistic approach. Most of the publications appear to investigate (sources of) cyber risks and how to tackle them, instead of focusing on the foundational elements of **C-SCRM** in an integrated way (Creazza et al., 2022). Boyens et al. (2021) and Boyson et al. (2022) find that the effective implementation of **C-SCRM** practices remains inconsistent and organisations still continue to face difficulties in acknowledging the challenge, determining an appropriate approach, and initiating action. A recent report by the European Union Agency for Cybersecurity (ENISA) highlights that organisations lack the necessary governance structures to manage risks in the **CSC** (Papaphilippou et al., 2023). Most importantly, the implementation seems to fall behind the pace of threat dissemination (Boyson et al., 2022). The non-standardised nature of **C-SCRM** poses additional difficulties in implementing sound mitigation measures (Boyson et al., 2022). Topping et al. (2021) state that existing frameworks and methodologies lack commonality and alignment as they address different categories and various levels of detail. Literature seems to incorporate a wide range of topics in the field, however, without any holistic view that enables coordination mechanisms between them (Creazza et al., 2022). Further, many contributions lack the definition of the elements that make up the **CSC**, which are crucial for effectively managing risks associated with it (Topping et al., 2021).

All in all, the reviewed literature shows that there is a lack of what elements complement and facilitate success towards a holistic **C-SCRM**, and guidance is missing on what organisations need to do to extend their **C-SCRM** beyond the scope of their firm (Colicchia et al., 2019; Topping et al., 2021). Comprehensive studies and holistic, theoretically grounded frameworks are needed (Garvey et al., 2021; Colicchia et al., 2019).

1.1.4 European and National Regulation

Beyond the current push for companies to get a handle on their SC cybersecurity, binding European regulation is on the way that will make organisations even more accountable. Here, we are speaking of the already published **NIS2 Directive**, which will become binding in all EU member states in October 2024, as well as the upcoming **CRA**, which is estimated for 2025/2026. This subsection will mainly focus on these two EU regulations while adding some brief indications of further EU and national regulations at the end. On the way to tackle current fragmentation in EU cybersecurity law and towards a comprehensive EU cybersecurity framework, in particular the interplay between the new regulations is of interest. The studies of Eckhardt and Kotovskaia (2023) and Chiara (2022) have investigated these points of (dis)interaction in detail, which are summarised below focusing on the aspects of SC cybersecurity. Both regulations also intersect with other more specialised or sector-specific regulations, which will not be covered in the subsequent part of this work.

From a holistic point of view, the **NIS2** aims to enhance the cybersecurity level of critical services provided by public and private entities essential for societal functioning, while the **CRA** emphasises measures to enhance the level of cybersecurity of hardware and software products, also called *products with digital elements*. In practice, this implies that organisations will have to take technical, operational and organisational measures in all perspectives of cybersecurity to manage risks of the network and information systems they use. The **CRA**, on the other hand, will require manufacturers and distributors of products with digital elements to deal with vulnerabilities of their products throughout design, development, manufacturing and even after placing them on the market. Parts of the requirements of **NIS2** address cybersecurity risks in SCs of the affected organisations as well as the relationships with their partners. Those measures will target the connections with firms *direct* suppliers and service providers and their contractual agreements. Thus, one limitation of **NIS2** will be the exclusion of sub-suppliers. To release the sole responsibility of entities at the end of the chain, the **CRA** makes manufacturers and distributors accountable for delivering products with an appropriate level of cybersecurity and in a secure default configuration. Corresponding conformity assessments will be used to ensure compliance. Therefore the **CRA** will serve as a mechanism to prevent scenarios where even sound risk management processes fall short of ensuring an adequate level of organisational security due to the market for products not adequately meeting the security needs of organisations. Additionally, the transparency requirements of the **CRA** will require manufacturers to provide technical documentation that can be used to make informed acquisition decisions according to the requirements of procurement departments. The lifecycle approach as described earlier, will also ensure access to timely security updates. Furthermore, the **NIS2** and the **CRA** proposal collaborate in conducting coordinated risk assessments on critical ICT services, systems, and products in SCs through the "Cooperation Group", where the product categorisation of the **CRA** might be leveraged. All in all, the requirements of the **CRA** will support organisations to deploy their ICT products more securely and might help them to comply with the requirements of the **NIS2** in regards to SCs.

Taking a closer look at the developments in the Dutch regulatory landscape reveals a proactive approach regarding the implementation of the **NIS2 Directive**. The *Netherlands Cybersecurity Strategy 2022-2028* (2022b), released in October 2022, along with the subsequent action plan (2022a), offers insights into how the Netherlands envisions its transition to a secure digital society. Two of the four pillars in the new strategy directly tackle SC risks. The primary focus of the **NIS2** lies in the first pillar titled *"cyber resilience of the government, businesses and civil society organisations"*. Just as the first **NIS Directive**, the Dutch government plans to implement the new **NIS2 Directive** within the ***Wet beveiliging netwerk- en in-***

formatiesystemen (WBNI), which regulates providers of essential and digital services. Moreover, plans are in place to integrate the **NIS2** into the ***Baseline Informatiebeveiliging Overheid (BIO)***, detailing security requirements for government organisations, where applicable. In this context, it is also worth noting that the implementation of sectorial legislation like ***Digital Operational Resilience Act (DORA)***, which poses important requirements in regard to SC cybersecurity towards organisations operating in the financial sector, and related regulations like the ***Critical Entities Resilience Directive (CER)*** will be closely coordinated. The revision of the **critical infrastructure policy** in light of the new regulation has also been announced by the government. Especially in the cyber resilience of the infrastructure and water management sectors, the strategy drives increasing sector-specific initiatives to understand SC risks. Another key pillar of the strategy is dedicated to examining SC cybersecurity from a product standpoint, aiming to "secure and innovate digital products and services". The action plan underscores the Dutch government's pressing support for the CRA negotiations, emphasising the need for its harmonisation with other sector-specific legislative frameworks of products and services.

1.2 Research Questions and Objective

A variety of publications prior to this study have investigated the nature of cyber risks in the SC as well as strategies, practices, and control frameworks to mitigate them. However, the implementation of a C-SCRM beyond the focal firm as well as leveraging organisational foundations for sustainable success remains unexplored. Thus, the research objective of this study is to examine the current state of implementation in the Netherlands and explore the structural elements and organisational drivers of C-SCRM.

Therefore the following main research questions are defined:

RQ1: *Which primary research topics and concepts about C-SCRM have been investigated in prior research?*

RQ2: *What are structural elements and drivers for successful implementation and operation of an organisational C-SCRM?*

RQ3: *What is the operational state of C-SCRM in organisations within the Netherlands?*

RQ4: *How are the structural elements and drivers for C-SCRM perceived in practice?*

1.3 Research Design

The research uses a variety of methods to answer the defined research and knowledge questions. In this section, we introduce the overall methodology as well as an overview of the used methods. The methods are further explained in the respective chapter where it is applied. A summary of the research design can be found in Figure II.

1.3.1 Methodology & Methodological Fit

The purpose of this study is exploratory. As Saunders et al. (2019b) state, exploratory research is particularly useful to clarify the understanding of yet not precisely explored problems or phenomena. Thus, exploratory research seeks new insights and assesses phenomena in a new light (Makri & Neely, 2021). Although the notion of the SC and SC risk management are well researched, the application in the context of C-SCRM

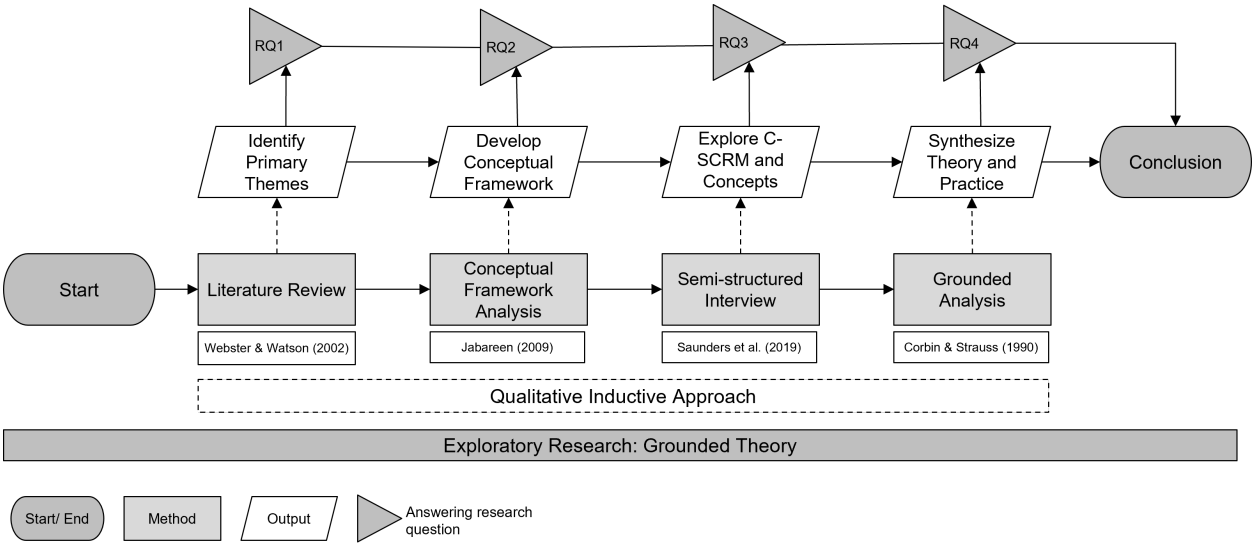

FIGURE II. Overview of research design and used methods. Own illustration.

remains relatively new. By exploring the structural elements and drivers for organisations implementing C-SCRM the study investigates known concepts in a new context. To facilitate this purpose the study uses grounded theory as a systematic research methodology for exploration and explanation of new theory through the categorisation of data. Grounded theory is especially used to generate theory that explains at a broad conceptual level an interaction about a substantive topic (Creswell, 2012; Makri & Neely, 2021). It, therefore, uses concepts as the basic units of analysis. Specifically, an inductive approach is chosen, meaning that initial data is collected first for the subsequent work. This approach suits best in cases where only little theory exists, as in the case of C-SCRM (Makri & Neely, 2021).

1.3.2 Methods

To facilitate the qualitative inductive grounded theory approach this study uses different methods. The initial data collection is done through a concept-centric literature review using Webster and Watson (2002). The following conceptual framework is developed under orientation on the conceptual framework analysis method by Jabareen (2009). To explore the established framework and subsequent concepts in practice, semi-structured interviews are a suitable method for data collection (Makri & Neely, 2021). The interviews are planned and executed following the guidance of Saunders et al. (2019a). Finally, the data is analysed using the classical Grounded Analysis for Grounded Theory by Corbin and Strauss (1990). The Grounded Analysis consists of the four steps of open coding, axial coding, selective coding and theory writing. The process is supported by using the qualitative data analysis software *Atlas.ti*. The implementation of the methods is further described at the beginning of the chapters where it is applied.

1.3.3 Research Quality and Validity

To ensure the research quality and validity this study uses the criteria by Guba (1981), emphasised by Makri and Neely (2021). All of the criteria are reviewed frequently throughout the process of writing this thesis.

Internal Validity

Internal validity or credibility reflects the degree to which the results accurately reflect the perspectives of the individuals involved rather than the researcher's biases (Makri & Neely, 2021). To ensure credibility, the interviews are promptly evaluated using a consistent approach. Moreover, the research guarantees the inclusion of data gathered from different sources by selecting participants from various sectors, roles/functions, and varying levels of experience. Especially for C-SCRM, participants are selected from sectors representing different actors in the SC, research organisations as well as federal organisations.

External Validity

External validity or transferability ensures that the findings of the study can be used in other contexts (Makri & Neely, 2021). Therefore, besides the diverse choice of participants, this study aims to set the results into perspective with prior theory and, especially, aspires to guide future research by developing a holistic conceptual framework. The researchers are aware of the limitations of the study, which are described transparently in Section 1.4.

Reliability

Reliability or dependability refers to the degree to which the study can be repeated and replicated by other researchers (Makri & Neely, 2021). This is ensured through careful documentation and justification of the audit trail including illustrative examples. Besides this chapter, the study introduces selected methodologies and elaborates on their execution within the chapter they are applied. Therefore, a respective method section is introduced in the corresponding chapters.

Objectivity

Objectivity or confirmability refers to the extent to which the findings align with the gathered data and remain unaffected by the researcher's personal biases, ensuring the results derive solely from the data itself (Makri & Neely, 2021). To uphold this, the researchers regularly confer with the supervisors about evolving findings and next steps.

1.4 Scope

The scope of this thesis is twofold. First, the aim is to explore structural elements and drivers for holistic and organisational C-SCRM. The study uses prior publications around organisational C-SCRM programs and governance structures as well as grey literature in the form of reports and governmental publications. Specific use cases of technologies or methodologies to mitigate certain cyber risks are not considered. To close the described research gap for a more holistic perspective, the study establishes a conceptual framework that can be leveraged by research and practice to conduct further studies in detail. The study does not aim to define a methodology to implement a C-SCRM but rather investigates specific concepts within an organisation or its ecosystem that influence the development and operation. Second, the study aims to explore the current state of C-SCRM as well as the perception of the defined concepts in practice. The scope is limited to private and public organisations operating in the Netherlands. Thus, the semi-structured interviews do not aim to precisely validate the conceptual framework due to the complexity and the number of concepts. Therefore the interviews aim to investigate the concepts in more detail and give an overview

of how experienced experts perceive their relevance and maturity in practice to guide future research and present an overview and tailored insight for practitioners. Furthermore, the number of participants does not allow for any quantitative conclusions regarding successful implementation strategies for C-SCRM.

1.5 Structure

The thesis is structured as follows. In Chapter 1 we gave a short introduction. The Background provided more information on the complexity of SCs, recent SC attacks, the emergence of C-SCRM, and the influence of current and upcoming regulation. Further, we introduced the research design, followed by the scope of this study and relevant definitions. In Chapter 2 we describe the results of the literature review, along with a detailed description of the used methodology. The literature review will address research question RQ1 and RQ2. In Chapter 3, we introduce the interview method, followed by the elaborate description of the results and a revision of the conceptual framework in Chapter 4. The results are discussed in Chapter 5 and provide answers for research question RQ3 and RQ4. Chapter 6 concludes the thesis with theoretical and practical implications and limitations. In Chapter 7 we provide tailored recommendations. A detailed overview of the structure is given in Figure III. The figure also indicates the chapters, in which the research questions are addressed.

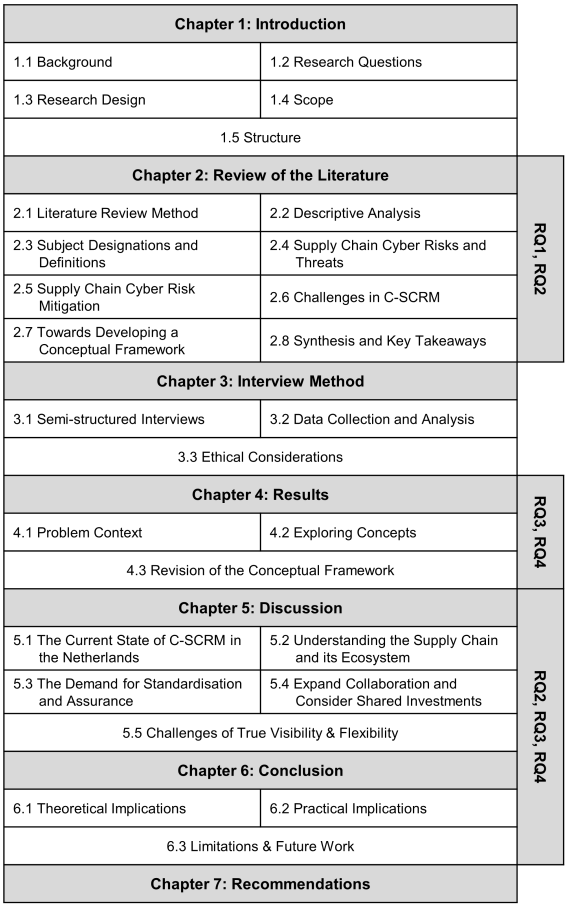

FIGURE III. Structure of the thesis. Own illustration.

2 | Review of the Literature

In this chapter, we carry out a literature review to establish an overview of relevant prior publications. First, we present the review method in Section 2.1, followed by a descriptive analysis in Section 2.2. The textual analysis and the corresponding findings are presented in Sections 2.3 to 2.6. In Section 2.7 we define and present the initial conceptual framework. This chapter is concluded in Section 2.8.

2.1 Literature Review Method

A literature review helps to facilitate theory development by utilising existing research while uncovering areas where more research is needed (Webster & Watson, 2002). A concept-centric approach is chosen as according to Webster and Watson (2002), an author-centric approach fails to synthesise the literature. Thus, this review analyses existing literature and theories in the field of C-SCRM to define the central concepts and finally propose a conceptual framework to synthesise and extend existing research (Webster & Watson, 2002). The framework is constructed with orientation on the eight-step methodology by Jabareen (2009). Therefore, the review addresses the corresponding research questions RQ1 and RQ2. This section will further elaborate on the steps undertaken within the review.

Identifying Relevant Literature

A thorough literature review should consider all relevant scientific studies on the topic, without being limited to a specific research approach, a particular group of journals, or a specific geographical location (Webster & Watson, 2002). To identify all relevant contributions, a structured three-step process is carried out.

First, a main query for use within the *Scopus* database is tested and defined. The main goal here is to cover the main body of publications specifically in the field of existing C-SCRM literature. The following query was identified as delivering the most comprehensive results with a total of 270 publications:

> TITLE-ABS-KEY((((ict OR cyber) AND ("supply chain" OR "supply-chain")) AND risk AND management) OR "ICT-SCRM" OR "C-SCRM" OR "CSCRM" OR "SCCRM")

The publications derived from the query are first assessed based on a title and abstract. After excluding all articles that do not address the research goal, a full-text screening is performed to identify the articles that will be included in the study.

Second, as proposed by Webster and Watson (2002), forward and backward searching (snowballing) is an excellent way to elicit further publications. Therefore, it was used to complement the review. Furthermore, the field of C-SCRM consists of major contributions from governments and industry. The most popular pieces of grey literature are carefully selected and included.

Third, to ensure to not miss any relevant publications closer to the broad field of SC risks, another more general query is defined. With a total of 1.577 results, the query was further specified using exclusion

criteria. To keep this research relevant, papers published before 2020 are excluded. Further, only publications in English of type articles, books (chapter), reviews and conference proceedings are considered. Finally, literature from non-relevant disciplines like social science, physics and astronomy are excluded, leaving a total of 671 results. The query can be found below. Literature retrieved from this query is also considered under the results of "snowballing".

> TITLE-ABS-KEY (((ict OR cyber OR digital) AND ("supply chain" OR "supply-chain") AND risk* OR threat* OR attack* OR vulnerab*))

The explained steps and corresponding results are summarised in the flowchart in Figure IV.

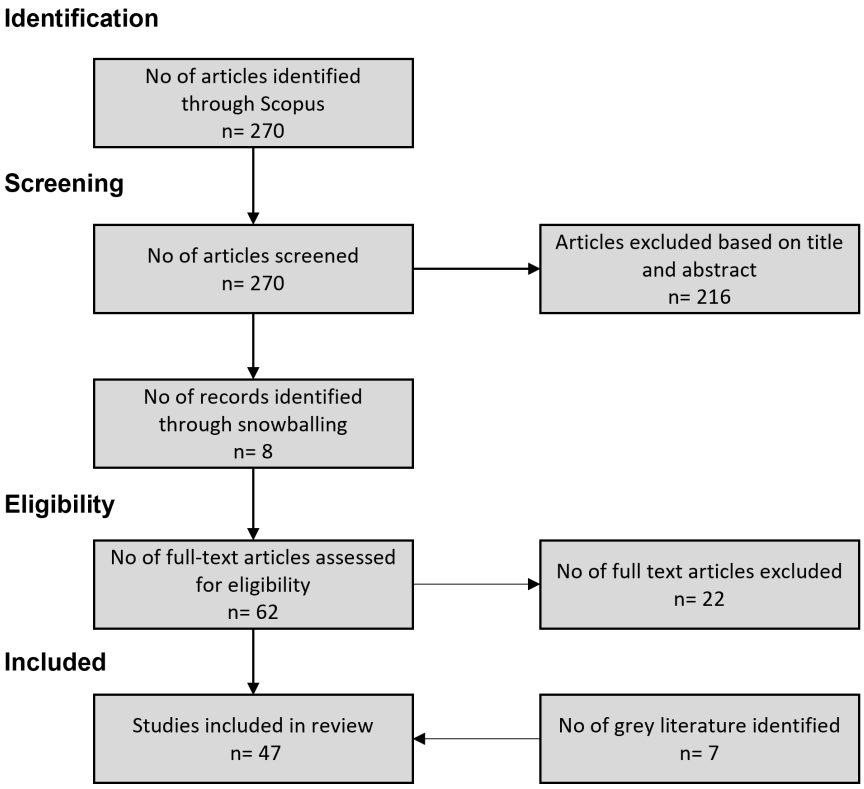

FIGURE IV. Literature identification and screening process. Adapted from Moher et al. (2009).

Analysing Relevant Literature

To analyse the relevant literature, we carry out a descriptive analysis first, to identify key trends in the considered publication timeline. Following up, the textual analysis will identify key themes within the field and present them in a concept-centric manner. Finally, a review should identify critical knowledge gaps and thus motivate researchers to close this breach with future research (Webster & Watson, 2002). This is supported by the construction of a conceptual framework. This research orientates on the methodology of Jabareen (2009) and consists of the following steps: Mapping the selected data sources, extensive reading and categorising of the selected data, identifying and naming concepts, deconstructing and categorising the concepts, integrating concepts, synthesis, resynthesis and making it all make sense, (validating) rethinking the conceptual framework.

2.2 Descriptive Analysis

Before continuing with the textual analysis, we give a brief, descriptive overview of the selected literature in this section. Figure V shows the number of articles selected for this study between the years 2012 and 2023 (excluding Warren and Hutchinson (2000)). Although multiple authors mark Warren and Hutchinson (2000) as the primary study acknowledging the concept of the CSC, the majority of publications first addressing the described problem were published in 2012. After a decrease in publications between 2015 and 2018, a significant rise within the past three years can be observed, which seems to continue in 2023. The trend emphasises the rising attention to the topic. When looking at the different journals of the selected publications, the multifaceted nature of the discipline becomes visible. These exemplary include journals on transportation, logistics, operation, critical infrastructure protection, information systems, and computer science. Most identified studies are qualitative, which is seen as an indicator of the immaturity of the field and a lack of key concepts (Ghadge et al., 2020). This is further emphasised by the different terms used in titles and keywords. Thus, most studies are conceptual and make use of surveys and interviews. Table II provides an analysis of all studies included. To complement the academic literature, this study incorporates carefully selected grey literature. The selection, mainly including NIST publications, is shown in Table I.

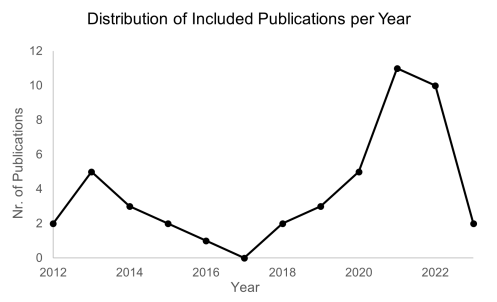

FIGURE V. Overview of included publications per year. Own illustration.

TABLE I. Overview of used grey literature.

Author	Institution	Publication
van den Brink et al. (2021)	TNO	TNO 2021 R10245 - Issues and perspectives for ICT SCRM - an initial exploration
ENISA (2021)	ENISA	ENISA Threat Landscape for Supply Chain Attacks
Boyens et al. (2020)	NIST	Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations
Boyens et al. (2021)	NIST	NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
Boyens et al. (2022)	NIST	NIST SP 800-161r1 - Cybersecurity Supply Chain Risk Management for Systems and Organizations
Miller (2013)	MITRE	Supply Chain Atack Framework and Attack Patterns
Martin (2020)	MITRE	MITRE System of Trust™

TABLE II. Descriptive analysis of main contributions from literature.

Selected article	Research Methodology			Research Design				
Author et al. (year)	Qual.	Quant.	Mixed	Survey/ Interview	Case Study	Concept	Model\Simulation	Review
Bandara et al. (2021)	✓					✓		
Bartol (2014)	✓					✓		
Boyes (2015)	✓					✓		
Boyson et al. (2022)		✓		✓				
Boyson (2014)		✓		✓				
Cha (2022)	✓							✓
Cheung et al. (2021)	✓							✓
Colicchia et al. (2019)	✓				✓			✓
Creazza et al. (2022)		✓		✓				✓
Davidson and Shankles (2013)	✓					✓		
Deane et al. (2022)		✓		✓				✓
Fernando et al. (2023)		✓		✓				
Filho et al. (2021)	✓							✓
Gani and Fernando (2018)	✓							✓
Gani et al. (2023)		✓		✓				
Garvey et al. (2021)	✓							✓
Ghadge et al. (2020)	✓							✓
Guerra and Estay (2019)	✓					✓		✓
Hampton et al. (2021)		✓		✓				
Kim and Im (2014)	✓			✓				
Lu et al. (2015)	✓							✓
Ludvigsen et al. (2022)	✓							✓
Martínez and Durán (2021)	✓							✓
Masip-Bruin et al. (2021)	✓					✓		
Melnyk et al. (2022)	✓			✓				✓
Nygård and Katsikas (2022)	✓							✓
Pandey et al. (2020)	✓				✓			✓
Pérez-Morón (2022)	✓							✓
Sawik (2022a)	✓						✓	✓
Schauer et al. (2019)	✓					✓		
Shankles et al. (2013)	✓					✓		
Shoemaker and Mead (2013)	✓					✓		
Shoemaker and Wilson (2013)	✓					✓		
Shoemaker et al. (2012)	✓					✓		
Siciliano and Gaudenzi (2018)	✓			✓				
Sobb et al. (2020)	✓							
Topping et al. (2021)	✓							✓
Warren and Hutchinson (2000)	✓					✓		
Windelberg (2016)	✓					✓		

2.3 Subject Designations and Definitions

What stands out from the reviewed literature are the various terms and definitions used for both, CSC and C-SCRM. Not only does the literature differ in the use of terminology, but the authors are also addressing different perspectives. This results in the use of diverse terminologies to describe identical concepts, as well as the application of identical terminologies to refer to distinct concepts (van den Brink et al., 2021). As already described in Section 2.2, this phenomenon points to the infancy of the field and a lack of foundational studies, while also highlighting the complexity.

2.3.1 The Cyber Supply Chain (CSC)

Examples of other terms used for CSC are: "ICT Supply Chain", "Digital Supply Chain", "IT-Supply Chain", "IT-Enabled Supply Chain", "Virtual Supply Chain" or "E-Supply Chain" (Garvey et al., 2021; van den Brink et al., 2021). Furthermore, it is noticeable, that not all authors provide a sound definition for their terminology, which leads to the emergence of different, not aligned research streams, not leveraging

prior research most effectively. Garvey et al. (2021) point out the general problem within the field, namely that it seems like "many have been defining the tools of the trade without first defining the trade". Table III gives an overview of the various definitions present in the literature.

TABLE III. Definitions of the CSC and related terms.

Author	Definition
Cyber Supply Chain	
Boyson (2014)	...the entire set of key actors and their organisational and process-level interactions that plan, build, manage, maintain, and defend the IT system infrastructure.
Kim and Im (2014)	....a supply chain enhanced by cyber-based technologies to establish an effective value chain.
Ghadge et al. (2020)	...a network of IT infrastructure and technologies that are used to connect, build and share data in virtual networks
Garvey et al. (2021)	The cyber supply chain of a focal firm is the collection of nodes and linkages that compose of cyber assets, that are in either the product or support supply chain, that are directly or indirectly connected to cyberspace.
Other	
Lu et al. (2015)	*ICT Supply Chain* refers to the full set of key actors included in the network infrastructure, including end-users, policymakers, procurement specialists, systems integrators, network providers and software/hardware vendors.
Sobb et al. (2020)	*Supply Chain 4.0* is the physical and technological integration of systems across networks, which allows increased production, organisation and profitability, characterised by autonomous actions independent from the location, prevalent integration, various automated services, and by its ability to react context to the customers' needs and requirements.
Boyson et al. (2022)	*A Digital Supply Chain* is a highly integrated global internet community of customers, distributors, producers, and suppliers whose order signals, production/warehouse systems, and inventory tracking/delivery field sensor devices are linked together across a shared network.

The definition of the CSC has expanded over time, similar to how the entire field has broadened in its scope. One of the early definitions of the CSC is provided by Boyson (2014)[1], which is widely used in later publications like e.g. Pandey et al. (2020); Fernando et al. (2023); Gani and Fernando (2018). It can be seen that, depending on the aim of the study and its publishing sector, the authors set a different focus. Mainly early studies address the ICT-product SC (e.g. Lu et al. (2015); Shoemaker and Mead (2013); Shoemaker and Wilson (2013); Davidson and Shankles (2013); Shoemaker et al. (2012); Shankles et al. (2013); Masip-Bruin et al. (2021)) to enhance product integrity and gain visibility into the vast amount of suppliers contributing to a final ICT product. Other studies, mainly from logistics, set the focus on technology-enhanced "physical" or "core business" SCs to increase their efficiency and profitability through e.g. collaboration or automation (e.g. Sobb et al. (2020); Boyson et al. (2022); Gani and Fernando (2018); Ghadge et al. (2020)).

However, to combat the growth of definitions, this work will adopt the viewpoint of Garvey et al. (2021), which in the scope of this study has been identified as the most advanced definition, incorporating a fusion of the definitions mentioned prior. For an element to be part of the CSC, two criteria must be fulfilled. For the

[1]The definition stems from an earlier work of the author in 2009, which at the time of writing is not available anymore.

first criterion, the study extends the SC theory by Carter et al. (2015), which argues that a SC consists of a product (movement of a product of any kind between SC nodes) and a support layer (supporting a product SC) by adding a third, intertwined layer: the cyber layer. This layer can include ICT components or services used in any SC process (product) or firms that supply these components. Therefore, an element has to be part of either the product or support the SC. Second, the element has to be connected to cyberspace, physical or virtual (Garvey et al., 2021). Thus, the final working definition of the CSC, as briefly introduced in Section 1 is:

> ***The Cyber Supply Chain of a focal firm is the collection of nodes and linkages that compose of cyber assets, that are in either the product or support supply chain, and directly or indirectly connected to cyberspace (Garvey et al., 2021).***

2.3.2 Cyber Supply Chain Risk Management (C-SCRM)

Similar to the definition of the CSC, C-SCRM is also subject to various interpretations. Filho et al. (2021) is the first study that differentiates between two research streams, which are further categorised by Cha (2022) as being either product-centric (ICT SC risks) or process-centric (risks generated by the use of technology along the SC). Thus, parallels to the definition of the CSC can be identified. Due to the complexity of SC risks, the collaboration of professionals, who previously had no experience working together (e.g. IT, Risk, SC), is required to break down significant differences in culture and language (Bartol, 2014; Boyson, 2014) and therefore explains the variety of topics and the emergence of different streams in the field.

Melnyk et al. (2022) describe the current state of research in the field by using an accurate metaphor derived from a poem by Saxe (1872): *"In this parable, six blind men are introduced to an elephant – an animal that they have never met before. Each person touches a different part of the elephant; each comes away with a different view of what the elephant is. Each view is simultaneous right and, because it is incomplete, also wrong."*

This resulted in the use of different terms next to C-SCRM e.g. "Supply Chain Cyber Risk Management (SC-CRM)", "ICT-SCRM", "Cybersecurity across the supply chain (CSAC)" or "Supply Chain Cybersecurity". Table IV shows some of the different views on C-SCRM. Similar to the definition of the CSC, this research aims for a holistic approach, combining disparate views. This review adopts the term C-SCRM introduced by NIST to support the establishment of a unified terminology but doesn't intend to only point and build up on the corresponding publications *NIST SP 800-161r1* and *NISTIR 8276*. Therefore it combines the interpretations of Boyson (2014); Melnyk et al. (2022); Garvey et al. (2021) towards the following working definition:

> ***"Cyber Supply Chain Risk Management (C-SCRM) is a holistic system approach with programmatic activities, including strategies, policies, technology, processes and people to assess and mitigate risks in the Cyber Supply Chain, associated with the possible loss or damage of cyber assets, resulting in the possible disruption of any supply chain process."***

TABLE IV. Definitions of C-SCRM and similar concepts.

Author	Definition
Cyber Supply Chain Risk Management (C-SCRM)	
Boyson (2014)	...defined as the organisational strategy and programmatic activities to assess and mitigate risks across the end-to-end processes (including design, development, production, integration, and deployment) that constitute the supply chains for IT networks, hardware, and software systems.
Boyens et al. (2022)	.... a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.
Fernando et al. (2023)	...a strategic management activity to prevent current and future cybersecurity threats.
Other	
Davidson and Shankles (2013)	*Information and Communication Technology Supply Chain Risk Management (ICT-SCRM)* seeks to manage and mitigate cyber and supply chain risk throughout an acquisition and sustainment lifecycle for an element or a system.
Melnyk et al. (2022)	*Cybersecurity across the supply chain (CSAC)* is defined as a holistic, systems approach that draws upon technology, procedures, and people to protect networks, systems, devices and digital assets from damage, attack, or unauthorised access due to agents and/or organisations targeting and exploiting (directly or indirectly) weaknesses in the supply chain network.
Garvey et al. (2021)	*Supply Chain Cybersecurity* is the collection of strategies, policies, and processes that manage and mitigate against the possible loss of cyber assets and the possible subsequent disruption of any supply chain process that manifests as a result of the loss of a cyber asset.

2.4 Supply Chain Cyber Risks and Threats

Before one can investigate how to mitigate risks in the CSC, it is crucial to understand the different types of risks. Divergent perspectives on potential risks can create discrepancies in the SC, resulting in a decline in overall security effectiveness (Creazza et al., 2022). Literature covers different concepts describing CSC risks, summarised in Table V. It is noteworthy to mention that in some studies, the meanings of words like threat, vulnerability, and risk are different from their traditional definitions in the field of information security. In this section, we summarise the different concepts, derived from the literature.

Authors have different opinions on what to consider to be a CSC risk. Filho et al. (2021) argue that one should not focus on the type of SC (e.g. CSC), but attention should lie on the source of risk. This review defines a SC cyber risk as any potential harm or compromise that may arise from suppliers, their SCs, their products, or services (Boyens et al., 2022). Further, for an attack to be considered a SC attack, it has to be a combination of two attacks, first on a supplier, that is then used to attack the main target (ENISA, 2021).

Types and sources of cyber risks are often investigated interchangeably. Ghadge et al. (2020) define a classification of types of cyber risks and map the most common attack methods or threats. The classification includes physical threats, breakdown, indirect attacks, direct attacks, and insider threats. Others are classi-

TABLE V. Researched concepts of cyber SC risks.

Concept	Author
Type of cyber risks	Pandey et al. (2020); Ghadge et al. (2020); Boyens et al. (2022); Pérez-Morón (2022)
Sources of cyber risk	Colicchia et al. (2019); Pandey et al. (2020); Creazza et al. (2022); Pérez-Morón (2022)
Threats	Shoemaker et al. (2012); GAO (2012); Davidson and Shankles (2013); Boyson (2014); Filho et al. (2021); Cha (2022); Lu et al. (2015); Boyens et al. (2022)
Attack strategies\techniques	Pandey et al. (2020); Ghadge et al. (2020); Nygård and Katsikas (2022); ENISA (2021)
Vulnerabilities	Schauer et al. (2019); Filho et al. (2021); Deane et al. (2022); Garvey et al. (2021); Boyens et al. (2022); GAO (2012)
Risk propagation	Ghadge et al. (2020); Garvey et al. (2021); Schauer et al. (2019)
Points of penetration	Ghadge et al. (2020); Filho et al. (2021); ENISA (2021)

fying different types of risks into e.g. supply risks, operational risks and demand/ customer risks (Pandey et al., 2020; Pérez-Morón, 2022), which aligns more with a SC perspective. Boyens et al. (2022) waive a classification and elaborate on the structure of risks by providing some practical examples. Sources of cyber risks are mostly divided into location, meaning internal (current/ former employees) or external (supplier-s/contractors, customers, competitors, hackers) and nature, meaning malicious or non-intentional sources (Colicchia et al., 2019; Creazza et al., 2022). Threats are also often mixed up with the types of risks or certain attack methods. Boyens et al. (2022) make a distinction between adversarial and non-adversarial threats. Non-adversarial threats include natural disasters, poor-quality products/services, or legal/regulatory changes. However, in a closer view of the CSC, the literature seems to focus mainly on adversarial threats. Summarised, the main threats towards a CSC identified are counterfeits, malicious tampering, insider threats, industrial espionage, service outage and information leakage (Shoemaker et al., 2012; GAO, 2012; Davidson & Shankles, 2013; Boyson, 2014; Filho et al., 2021; Cha, 2022; Lu et al., 2015; Boyens et al., 2022). However, the literature agrees on the human factor to be the biggest and most unpredictable threat as well as vulnerability, companies often do not consider it close enough (Ghadge et al., 2020; Creazza et al., 2022). In contrast, attack methods and techniques can be named precisely. Table VI provides an overview of common attack methods within SC attacks, based on the classification of ENISA (2021).

Vulnerabilities are less discussed in research in comparison to attack methods or risk types. However, they can have persistent negative impacts on an organisation's mission due to an ongoing decrease in service level or ongoing theft of intellectual property (Boyens et al., 2022). GAO (2012) lists some common examples and corresponding threats for federal ICT SCs. On a higher level Deane et al. (2022), point out four ways a firm can be subject to risk in a SC, making them also levels where different vulnerabilities exist. Apart from direct attacks, an attacker can leverage a breached SC member, using them as a partner vector. This is amplified when a partner acts as a custodian, holding another partner's data. Finally, a firm can be attacked by a partner actor using privileged information. The frequency and magnitude of attacks are thereby dependent on objective factors (type, main business) and relationship factors (Deane et al., 2022). Schauer et al. (2019) differentiate between confirmed vulnerabilities (e.g. listed in online repositories) and unknown, zero-day

TABLE VI. Overview of attack methods/ techniques to compromise a CSC.

Attack method/ technique	Author
Malware	Nygård and Katsikas (2022); Filho et al. (2021); Cha (2022); ENISA (2021)
Social engineering	Pandey et al. (2020); Nygård and Katsikas (2022); Filho et al. (2021); Cha (2022); Ghadge et al. (2020); Colicchia et al. (2019); ENISA (2021)
Denial of service	Pandey et al. (2020); Nygård and Katsikas (2022); Filho et al. (2021); Cha (2022); Ghadge et al. (2020)
Brute-force attack	Nygård and Katsikas (2022); ENISA (2021)
Password sniffing	Pandey et al. (2020); Cha (2022); Ghadge et al. (2020)
Exploiting software vulnerabilities	Nygård and Katsikas (2022); Ghadge et al. (2020); ENISA (2021)
Exploiting configuration vulnerabilities	Nygård and Katsikas (2022); ENISA (2021)
Physical attack or modification	Nygård and Katsikas (2022); Ghadge et al. (2020); ENISA (2021)
Counterfeiting	Nygård and Katsikas (2022); Cha (2022); Ghadge et al. (2020); ENISA (2021)
Open-source intelligence	Nygård and Katsikas (2022); ENISA (2021)

vulnerabilities. Boyens et al. (2022) categorise vulnerabilities as either internal (e.g. vulnerable components, lack of awareness) or external (e.g. interdependencies, inadequate cyber hygiene). The reliable exploration of vulnerabilities remains difficult since the interconnectedness and possible cascading effects make it hard to determine whether an event occurred as a direct result of a SC vulnerability (Boyens et al., 2022). Garvey et al. (2021) and Schauer et al. (2019) suggest that vulnerabilities always have to be viewed from two perspectives. First, how a vulnerability can be exploited, and second, what other vulnerabilities can the attacker potentially reach after successfully exploiting the first one?

Furthermore, the literature discusses areas where cyber risks can enter an organisation's environment, also known as points of penetration or entry points. This information can help organisations focus their security efforts in the right places (Ghadge et al., 2020). Ghadge et al. (2020) take a holistic view and define technical, human, and physical points of penetration. ENISA (2021) details this view a bit more precisely, by explicitly naming supplier and customer assets that might be targeted. Against that, Filho et al. (2021) take more of a SC perspective and investigates material, information, and financial flows and stocks as entry points for cyber risks. Finally, some authors investigate cyber risk propagation, emphasising that CSC risks are not static and may propagate from their occurrence to other areas accompanied by cascading or ripple effects (Ghadge et al., 2020). Although, many authors acknowledge the challenges and uncertainties about risk propagation, only a few try to address and conceptualise it. Ghadge et al. (2020) define three propagation zones: primary propagation within the focal company, resulting in disruption of the operation. Secondary propagation within the SC network will incur near-time opportunity costs as well as long-term reputational damage. Tertiary risk propagation could substantially harm society when e.g. relevant to public health or basic utility. The impact of the in Subsection 1.1.2 described breach on 3CX underscores the potential consequences of cascading effects.

All in all, cyber risks in SCs are a much-researched topic, and of major importance for organisations to understand their attack surface. However, the inconsistency in the terminology and interpretation fails to provide a sound baseline. Creazza et al. (2022) find that risks are generally stronger perceived by the impact rather than the probability. This means that awareness of risks is influenced by their actual occurrence and little awareness leads to potentially underestimating the importance of risks, and vice versa. Therefore, incident management and building awareness are essential capabilities when dealing with cyber risks in SCs (Creazza et al., 2022).

2.5 Supply Chain Cyber Risk Mitigation

This subsection elaborates on academic and practitioner efforts to mitigate the aforementioned cyber risks. Therefore, three main concepts are identified. Mainly earlier research focuses on leveraging existing standards for C-SCRM. Another part of the publications provides different methods e.g. risk analysis as well as (conceptual) frameworks. Finally, a large amount of the reviewed studies identify and categorise specific best practices and mitigation measures for organisations to implement. Table VII provides an overview of the corresponding studies. In the following, we briefly elaborate on each of the three concepts.

TABLE VII. Researched concepts of CSC risks mitigation.

Concept	Author
Standardisation efforts	Shoemaker et al. (2012); Shoemaker and Mead (2013); Shankles et al. (2013); Davidson and Shankles (2013); Bartol (2014); Lu et al. (2015); Boyens et al. (2022)
Methods/ Frameworks	Windelberg (2016); Siciliano and Gaudenzi (2018); Guerra and Estay (2019); Schauer et al. (2019); Melnyk et al. (2022); Boyson et al. (2022); Gani et al. (2023); van den Brink et al. (2021); Boyens et al. (2022); Martin (2020); Miller (2013); Pandey et al. (2020); Ghadge et al. (2020); Fernando et al. (2023)
Best Practices/ Mitigation Measures	Boyson (2014); Ghadge et al. (2020); Colicchia et al. (2019); Creazza et al. (2022); Cha (2022); Cheung et al. (2021); Gani and Fernando (2018); Boyens et al. (2021, 2022)

Along with the description in Section 2.3 about the ICT SC, early efforts to develop safeguards for organisations mainly consisted of "mapping anything and everything" from available standards in information security and system and software engineering (Bartol, 2014). This led to the first constructs of requirements mainly retrieved from standards about software system lifecycle processes (ISO 12207-2008/ ISO 15288:2008) (Shoemaker & Wilson, 2013; Shoemaker & Mead, 2013; Bartol, 2014) and lifecycle process risk management (ISO 16085-2006) (Shoemaker & Mead, 2013). Additional requirements were retrieved from general information security standards (ISO 27k, NIST SP 800-53) and the NIST practices on SC risk management practices for federal information systems (NISTIR 7622) (Bartol, 2014; Shoemaker & Wilson, 2013). This means that various groups with different areas of expertise and viewpoints began to initiate standard development creating compartmentalisation. However, it also became clear that the discipline does not require the sum of all related disciplines, resulting in an emerged consensus of core and additional practices in the form of control frameworks (Bartol, 2014). Finally, after standardisation efforts within the literature slowed down, the NIST

special publication SP 800-161r1, which was recently revised, is seen as the "gold standard" for C-SCRM.

In scientific and practitioner literature, many different methods and frameworks have been introduced for various purposes and audiences with varying scopes. There are some publications, dealing explicitly with SC risks. Schauer et al. (2019) develop an evidence-driven risk assessment methodology for maritime SCs. Miller (2013) presents a SC attack framework and provides a catalogue with attack patterns. MITRE recently published its System of Trust™ framework which, accompanied by a tool, integrates evidence of organisational, technical, and transactional trustworthiness for decision-makers. The SoT has four main objectives, which include gathering and organising concerns surrounding trust, capturing evidence of trustworthiness, tailoring the system to specific concerns and questions, and implementing objective scoring mechanisms (Martin, 2020). A few authors have attempted to provide more holistic frameworks for C-SCRM. van den Brink et al. (2021) propose an analysis framework for the different perspectives of C-SCRM. Guerra and Estay (2019) develop a framework to mitigate the impact of attacks and present its application in an impact-wave analogy. Melnyk et al. (2022) conceptualise a research framework for the discipline and Pandey et al. (2020) present a framework of certain attack methods on information flows in SCs with corresponding mitigation strategies and Ghadge et al. (2020) define a so-called "SC cyber security system". Other publications are focusing on specific elements that facilitate security in CSC. Siciliano and Gaudenzi (2018) propose a framework to enhance the management of risks in SCs through resilience. Fernando et al. (2023) investigate the correlation between C-SCRM practices and SC visibility and Gani et al. (2023) dive into the relationship between information system security practices and SC performance. Windelberg (2016) proposes a set of objectives for managing CSC risks.

Finally, a variety of publications propose a set of organisational best practices or principles. Authors are attempting to categorise these best practices either along the phases of an attack (pre-, trans-, post-attack) (Creazza et al., 2022; Ghadge et al., 2020; Cheung et al., 2021) or on an organisational level (strategic, tactical, operational) Cha (2022); Boyson (2014); Boyens et al. (2022). Others choose to not use any categorisation (Boyens et al., 2021; Colicchia et al., 2019; Gani & Fernando, 2018). Existing literature points out that the majority of research is focusing on pre-attack measures, lacking guidance for the trans- and post-attack phase regarding e.g. real-time recovery and aftermath measures (Cheung et al., 2021; Ghadge et al., 2020).

2.6 Challenges in Cyber Supply Chain Risk Management

The management of risks in the CSC still poses some substantial challenges, both for organisations as well as for academic and practitioner research. The reviewed body of literature points out several areas for improvement and calls for further research. We briefly elaborate on the challenges and categorise them for a concise overview. Table VIII summarises the observed challenges.

Organisational challenges are meant to describe obstacles that firms face in implementing C-SCRM. Studies find that the general awareness of the problem is rising (Kim & Im, 2014). However, Siciliano and Gaudenzi (2018) report about a general misalignment between knowledge and action, meaning that decisions for C-SCRM are taken by roles with poor knowledge about IT and cyber risk and decision-makers fail to involve the right stakeholders e.g. IT managers in SC functions. On the other hand, preventive measures tend to rely too much on technological solutions and may fail to consider important factors like the impact on

TABLE VIII. Organisational and contextual challenges in C-SCRM.

Category	Challenge	Author
Organisational		
Awareness & knowledge	Misalignment in awareness	Siciliano and Gaudenzi (2018); Kim and Im (2014)
	Knowledge and skills gap	Ghadge et al. (2020); Garvey et al. (2021)
Communication, collaboration & alignment	Inter-organisational	Siciliano and Gaudenzi (2018); Ghadge et al. (2020); Masip-Bruin et al. (2021); Boyson et al. (2022); Nygård and Katsikas (2022); Sobb et al. (2020)
	Intra-organisational	Siciliano and Gaudenzi (2018); Ghadge et al. (2020); Colicchia et al. (2019)
Control & visibility	Vulnerabilities and propagation	Masip-Bruin et al. (2021); Nygård and Katsikas (2022); Colicchia et al. (2019)
	Security system complexity, dynamics and metrics	Masip-Bruin et al. (2021); Ghadge et al. (2020); Colicchia et al. (2019)
Contextual		
Lack of standard and regulation	Governmental involvement and guidance	Ghadge et al. (2020); Nygård and Katsikas (2022)
	Lack of standards and heterogeneous practices	Nygård and Katsikas (2022)
SC	Interconnectedness and complexity	Boyson et al. (2022); Garvey et al. (2021); Melnyk et al. (2022); Nygård and Katsikas (2022)
	Small and medium-sized businesses	Topping et al. (2021); Nygård and Katsikas (2022)
Research	Standardized terminologies and taxonomies	Bartol (2014); Topping et al. (2021)
	Lack of data and empirical studies	Ghadge et al. (2020); Cheung et al. (2021); Pandey et al. (2020)
	Limited body of research	Ghadge et al. (2020); Cheung et al. (2021)

investor reputation or the trustworthiness of suppliers (Siciliano & Gaudenzi, 2018). Next to that companies continue to suffer from the growing shortage of cybersecurity professionals (Ghadge et al., 2020; Garvey et al., 2021). The ISC (2022) reports a global gap of 3.4 million skilled cybersecurity professionals, growing twice as fast as the workforce. Ghadge et al. (2020) add that the current cyber threat landscape has clearly outpaced training efforts.

Another major challenge poses communication, collaboration, and alignment both, in the inter- and intra-organisational context. The prior challenge is thus somehow interrelated with the integration of internal processes and initiatives around C-SCRM, in other words, intra-organisational collaboration and alignment, which is of vital importance for a firm to take up with the complexity and interdisciplinarity. An even greater challenge poses collaboration between SC partners. Literature suggests, that SC partners should enhance transparency with each other regarding security and pool their security resources and know-how to tackle

the progressively complex cyber threats. Further integrating the SC through aligning systems and processes can lead to greater benefits such as standardised methods of working, common security objectives, and improved overall communication. (Ghadge et al., 2020) However, some suppliers may not be able to express their cybersecurity practices and reveal their SC information due to sensitive and confidential information, including competitive secrets and privacy concerns (Nygård & Katsikas, 2022).

A third main challenge faced by organisations is gaining control and visibility of the extended SC network. This includes the identification and management of the whole lifecycle of vulnerabilities and their propagation (Masip-Bruin et al., 2021). However, the limited availability of information about suppliers' SCs and the absence of e.g. centralised vulnerability repositories further hampers this and causes a lack of control (Nygård & Katsikas, 2022). Companies still struggle in the development of measurable, new security systems that meet the ongoing changing nature of cyber threats and are able to be coordinated by people with different skill sets in IT (Masip-Bruin et al., 2021).

Next to that, this work categorises contextual challenges, referring to pre-conditions and ongoing developments within the field, that pose difficulties for firms to implement a holistic C-SCRM. The structure and specific elements of a SC and therefore, as discussed before, the complexity and interconnectedness present a main challenge for organisations. Literature sees a general lack of standards and guidance within the field. Ghadge et al. (2020) argue that due to the complexity, more governmental involvement seems to be indispensable and Nygård and Katsikas (2022) question if the role of the change agent has to be taken up by the focal firm. This can be carried over to ongoing academic and practitioner research activities, which in general lack standardised terminology (Bartol, 2014; Topping et al., 2021). The limited body of research is further dominated by qualitative studies, due to the unavailability of cybersecurity data for proficient empirical studies. This further hampers research to determine the success of implemented C-SCRM practices (Ghadge et al., 2020). Authors are also arguing that this might be the reason why research is not progressing at the needed tempo, lacking behind the evolving attack surface (Cheung et al., 2021; Pandey et al., 2020).

Finally, some studies emphasise small and medium-sized enterprises (SME) as a key challenge, for successful C-SCRM, lacking attention in the current body of literature. This is confirmed by van den Brink et al. (2021), who report from several interviews that firms tend to focus on large suppliers, overlooking smaller links. Melnyk et al. (2022) argue that smaller organisations within SCs are often the most vulnerable, having weaker cybersecurity measures in place, due to limited financial and human resources. In contrast, they take over important roles in supplying niche products that are difficult to replace, while having disproportionate access to critical information in regard to their size. However, simply posing stricter cybersecurity requirements to SMEs may lead to supplier retention, due to their different structure or ability to implement measures. One observation from the Department of Defense in the US showed SMEs leaving the SC rather than complying after a newly released mandate, which would have incurred costs of over $3 million (Melnyk et al., 2022). Hence, larger enterprises need to seek out collaborative approaches that facilitate mutual support to enhance the security of their supply network sustainably.

2.7 Towards Developing a Conceptual Framework

This section proposes the conceptual framework based on the reviewed academic and practitioner literature. Some further specific research around the concepts is used for elaboration. The framework aims to structure the explored concepts that constitute the structural elements and drivers for an organisational, holistic

C-SCRM, on a strategic, tactical, and operational level (Multi-Level C-SCRM. The identified concepts are categorised into groups and mapped to their sources. The framework consists of four different groups. Therefore, the framework endeavours to explore the influence of various elements and drivers on the attainment of cyber assurance, -resilience, and -robustness through C-SCRM. By that, it follows, inter alia, the call for future research of Colicchia et al. (2019) and Garvey et al. (2021) and extends the initial work of Melnyk et al. (2022). Table A1 in Appendix A provides an overview of the element types and corresponding concepts derived from the initial literature review. The following will briefly introduce the element groups and corresponding concepts and provides some further elaboration from the literature to guide the subsequent research.

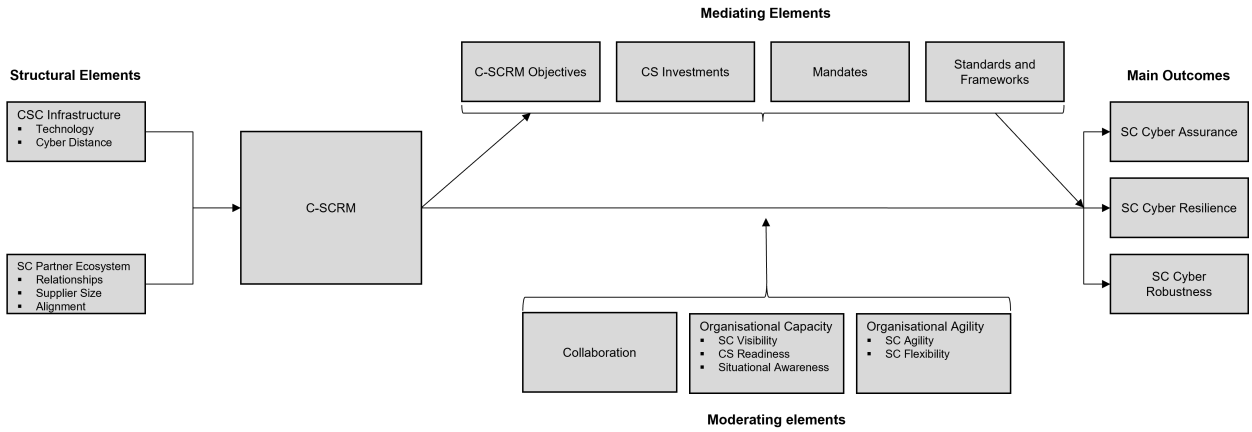

FIGURE VI. Conceptual framework - structural elements and drivers of C-SCRM. Own illustration.

2.7.1 Main Outcomes

The three main outcomes *SC Cyber Robustness, -Resilience, and -Assurance* have been found as the most named and desired outcomes of a C-SCRM program. These elements, therefore, function as the *dependent variables*, ideally being the result of a successfully running C-SCRM (*independent variable*). To examine the structural elements and drivers this study thus builds up on the cause-effect that a well-developed and operated C-SCRM leads to improved robustness, resilience, and assurance of the CSC.

SC Cyber Robustness

Cyber robustness represents the ability of the CSC to withstand any activity that aims to destructively alter an asset or deviate its operation from the planned operating state (Garvey et al., 2021). One could also explain cyber robustness as the outcome of classical "hardening" of the CSC. Thus, robustness majorly contributes to retaining the availability of the CSC (Alshurideh et al., 2023). In comparison to the manufacturing context, where robustness is often related to non-malicious errors or faults, cyber robustness is usually defined as the ability of an ICT system to resist intelligent, and goal-oriented attackers (Baiardi et al., 2016). Robustness involves various resources and capabilities within an organisation. The concept is not static and thus needs adjustments in response to both internal and external changes to continue functioning effectively (Küffner et al., 2022).

SC Cyber Resilience

The achievement of cyber resilience is the main object of discussion in various studies. There are various definitions of resilience in literature. Davis (2015) establishes three perspectives: one focuses on preparing for and reacting to incidents to minimise harm, while the other emphasises the ability of an organisation's IT to keep running despite errors or failures. Both perspectives are closely linked as organisations rely on IT for operations. Additionally, business continuity plans and disaster recovery are essential components of resilience, providing a framework for an organisation to plan and respond to incidents Thus, cyber resilience requires a combination of proactive and anticipating actions (Colicchia et al., 2019). As no system is ultimately secure, the critical capability for the CSC or a particular system is thus to respond and recover, or "bounce back" as fast as possible to its original or desired state and to adapt to manifested changes (Davis, 2015; Colicchia et al., 2019). SC cyber resilience and -robustness are very much interrelated. According to Wieland and Wallenburg (2013), resilience is achieved through robustness (proactive) and agility (reactive), with further enabling factors such as flexibility, SC visibility, and collaboration that help to facilitate the integration of cyber resilience into the SC.

SC Cyber Assurance

SC cyber assurance in the context of C-SCRM has become increasingly relevant within the past years. A limited body of research is investigating the rising need for how organisations can prove the robustness and resilience of their CSC towards the SC ecosystem. Hampton et al. (2021) find that the need for assurance is strongly influenced by the desire to enhance information about the SC partner and to verify the trust and commitment invested in them. The American Institute of Certified Public Accountants (AICPA) reacted to this demand and published a new assurance service in the form of a reporting framework for SCs. Thus it is assumed that clearly defined and documented C-SCRM processes will contribute positively to obtaining higher levels of assurance in the SC context.

2.7.2 Structural Elements

The structural elements in the conceptual framework represent the aspects that characterise the CSC, how it is organised (structured), and the nature of the participants that influence the context-specific development and decisions around C-SCRM. The study uses these elements to create awareness about the unique circumstances of each organisation and its SC ecosystem and to acknowledge that there is no "one-size-fits-all" for C-SCRM (Boyens et al., 2022).

SC Partner Ecosystem

The consideration of the different aspects of a *SC Partner Ecosystem* that a focal firm is operating in is of major importance. Here, the different types of relationships can substantially impact the initial situation. Ambrose et al. (2010) find that buyers and suppliers, in general, have different perceptions of their relationships while also recognising different drivers for a successful and sustainable relationship. Understanding these differences thus seems essential when approaching C-SCRM. As mentioned by Melnyk et al. (2022) and elaborated on in Section 2.6, especially the size of a firm operating in a SC plays a vital role. Finally, the level of internal and external alignment (also structural integration) prior to the establishment of a C-SCRM seems to have an important impact. Internal alignment refers to close collaboration and integration among different functions and departments. This allows better collaboration and thus, efficient engagement

in C-SCRM across the enterprise (Boyens et al., 2020). External alignment refers to the SC integration with partners in the ecosystem. Here C-SCRM focuses on establishing a relationship dimension to overcome the focus on single points along the interface of the SC (Creazza et al., 2022). All in all, these structural elements build the foundation of the environment, C-SCRM is built and operates on and is thus essential to be considered and understood (Melnyk et al., 2022).

Cyber Supply Chain Infrastructure

The CSC encompasses a variety of ICT systems, which can be integrated and used in organisational and SC processes in different manners. Therefore, the knowledge about which ICT systems a firm has to consider when trying to develop a C-SCRM is indispensable. In other words, analysing the composition of the CSC will give information on, inter, alia the attack surface a firm and its supply partners are facing. Thus, the element technology here refers to the number of different ICT components in the CSC. Additionally, the cyber distance further specifies how these systems are exposed to cyberspace, making them vulnerable to attacks (Garvey et al., 2021). Larger firms may have more complex ICT systems than SMEs and subsequently more ports are being exposed through collaboration with many suppliers (Wang, 2017). Adding up, the increasing integration and use of new disruptive technologies in SC processes like e.g. Internet of Things, cyber-physical systems or blockchain pose new and widely unknown vulnerabilities and ultimately cyber risk.

2.7.3 Mediating Elements

The mediating elements in the framework represent concepts, that are resulting from the development of C-SCRM and further detail how the main outcomes are achieved. As these elements partly represent more general cybersecurity concepts it is of major interest to investigate how they relate and benefit C-SCRM.

C-SCRM Objectives

As in traditional security programs a firm's initiative should be guided by overarching security objectives, that specify and guide all other measures below. The same applies for C-SCRM. Multiple authors argue, that the classic security objectives of confidentiality, integrity and availability, referred to as CIA-Triad are not sufficient to handle SC cyber risks (Windelberg, 2016; Boyes, 2015; Sawik, 2022a). They propose the use of the Parkerian Hexad to assess the SC from three angles: ensuring continuity of operations and safety, controlling access and system operations, and maintaining the accuracy and reliability of information and system configuration (Boyes, 2015).

Cybersecurity Investments

C-SCRM has to be supported by *cybersecurity investments*, aiming to protect an asset against a compromise in the area of set security objectives (e.g. Parkerian Hexad). The interconnected nature of SC cyber risks and the requirement to coordinate measures with SC partners implies that cybersecurity investments should be addressed for the entire SC (Sawik, 2022b). Thus, the main goal is to find a balanced way and make the right choices to invest in measures for implementation at different SC partners under a limited budget (Sawik, 2022a, 2022b). A study by Simon and Omar (2020) find that organisations that independently plan their cybersecurity investments often underinvest as they fail to account for the indirect damages suffered by their SC partners. They also find that it is indeed desirable for larger firms to invest in or subsidise

smaller firms' cybersecurity if they face high damage through a potential attack. Therefore, coordination mechanisms for cybersecurity investments should be considered in the development of C-SCRM.

Mandates

This study defines mandates as any requirement in the context of cybersecurity in the SC, issued either by the government or an organisation (e.g. SC partners). Melnyk et al. (2022) transpose the concept to C-SCRM from prior studies in the context of sustainability, retail and technology adoption. Consequently, there are two types of mandates: coercive pressure, which imposes negative consequences for non-compliance with the requirement, and signals, which convey the significance of a requirement and its associated behaviour or outcome. Next to (non-) compliance Melnyk et al. (2022) identify decoupling, where organisations create acceptance but fail to establish corresponding practices internally. Ultimately, strict requirements may cause a partner to drop out of the SC. Comparable scenarios are imaginable in the context of C-SCRM. Thus, the effect of mandates and subsequent behaviour of SC members is an important concept to be considered.

Standards and Frameworks

The use of established standards and cybersecurity frameworks in the SC context can assist in providing a common starting point, a common set of terminology, and a common understanding of how each partner approaches its cybersecurity (e.g. the multi-part ISO 27036) (Davis, 2015). However, Topping et al. (2021) find that the conflicting opinions on the composition of the SC and the effective management of cyber risks within it continue to hinder the development of a standardised and optimal approach to implementing a C-SCRM (indicated in the Background of this study). Davis (2015) suggests that it is possible to attain a certain level of protection upstream beyond Tier 1 partners, through the utilisation of flow-down controls, technical strategies, and regular auditing.

Next to the use of commonly agreed frameworks, standards might also be developed and applied in the context of a specific SC ecosystem. An illustrative example is Saudi Aramco, one of the largest global companies in the oil and gas industry, which, following a significant cyber attack in 2017, chose to create its own cybersecurity standard for third parties (SACS-002). This standard is being certified by several service firms to ensure compliance among relevant suppliers.

2.7.4 Moderating Elements

The moderating elements within the conceptual framework are concepts that affect the strength, also being the efficacy (effectiveness, efficiency), of the C-SCRM towards achieving the main outcomes.

Collaboration

Collaboration in the SC context is a widely-discussed concept to achieve resilience and has been identified as an integral enabler for successful C-SCRM by multiple studies e.g. Colicchia et al. (2019); Ghadge et al. (2020); Boyens et al. (2022). Collaboration in SCs includes may include different collaborative activities. Therefore, collaboration can be defined as responsible relationships among partners of a SC, who share information with each other and redesign business practices (Singh et al., 2018). Possible activities include information sharing, joint decision-making, incentive alignment, resource sharing, collaborative communication, or joint knowledge creation (Scholten & Schilder, 2015). These activities can be performed vertically with suppliers or customers as well as horizontally with competitors or other partners (Singh et al., 2018).

Collaboration's main benefits are increased effectiveness and efficiency for the SC (Singh et al., 2018). In cybersecurity, collaboration often involves threat information sharing enabling organisations to combine their knowledge, experience, and capabilities to gain a better understanding of the threats they face. By doing so, organisations can make threat-informed decisions on how to mitigate these threats (Johnson et al., 2016). A guide is e.g. provided by *NIST SP 800-150: Guide to Cyber Threat Information Sharing*. However, a number of barriers e.g. the establishment of trust, interoperability, and automation as well as how to safeguard critical information still pose difficulties in practice (Johnson et al., 2016).

Organisational Capacity

Cox et al. (2018) define organisational capacity as the enabling factors that allow an organisation to perform its functions and achieve its goals. This study uses the term to accommodate the concepts of SC visibility, cybersecurity readiness, and situational awareness that apply as enablers or at least influence the success of C-SCRM.

This study adopts the definition of SC visibility from Jüttner and Maklan (2011) as "the extent to which actors within the SC have access to or share timely information about SC operations, other actors and management which they consider as being key or useful to their operations". Within the context of C-SCRM, especially the knowledge about actors and cyber assets beyond tier 1 to which a firm's cyber SC is exposed are of main interest (Garvey et al., 2021).

Cybersecurity readiness is the level of an organisation's awareness, preparedness, and commitment to prevent and combat cyber-attacks (Hasan et al., 2021). As noted by Melnyk et al. (2022), the readiness not only of a focal firm but also of its suppliers and partners is essential to consider when implementing C-SCRM. Hasan et al. (2021) identify nine factors aligned to a firm's technological, organisational, and environmental context, while Melnyk et al. (2022) emphasise awareness, commitment, operational maturity, and resources for cybersecurity readiness.

Finally, situational awareness in the context of cybersecurity and SC plays a vital role. In this study, situational awareness includes the understanding of the "big picture" by establishing a common baseline of the current conditions available to partners and exchanged between them (Colicchia et al., 2019). Put simply, good situational awareness for C-SCRM includes the knowledge and understanding of potential cyber threats, vulnerabilities, and risks of the focal firm and its extended SC ecosystem (Guerra & Estay, 2019). Thus, this concept allows an organisation to act strategically and goal-oriented.

Organisational Agility

Agility is subject to various definitions, that summarised can be described as the reactive ability to answer to change (i.e. "react", "respond", "adapt", "re-configure") (Wieland & Wallenburg, 2013). This study uses the term organisational agility to accommodate the two concepts of SC agility and SC flexibility concerning C-SCRM.

The distinction between these two terms is not always clear. Generally said, the two concepts refer to an organisation's ability to respond to internal and external uncertainties via the integration of SC relationships. Agility refers to the strategic ability for a rapid response while flexibility refers to the operational ability for efficient change in the SC (Fayezi et al., 2017). In other words, agility conceptualises the "speed" for change, while flexibility draws on the "ease" of rearranging the SC. Thus, this study groups these terms as the ability to rearrange and alter relationships and dependencies in the current SC structure.

2.8 Synthesis and Key Takeaways

In this chapter, the most researched themes around C-SCRM were synthesised and conceptualised. The aim was to combine the existing perspectives and thus contribute to a commonly shared paradigm within the field and for the remainder of this thesis. Using the concept-centric approach by Webster and Watson (2002), the review conceptualised the various subject definitions, CSC risks and threats, CSC risk mitigation strategies, and C-SCRM challenges. Furthermore, a conceptual framework was proposed. The framework introduces the main concepts, presenting structural elements and drivers to achieve SC Cyber Robustness, -Resilience, and -Assurance by establishing an organisational C-SCRM. The concepts are grouped into structural-, mediating-, moderating elements, and main outcomes. The proposal of the conceptual framework majorly follows the research call of Colicchia et al. (2019) and Garvey et al. (2021) and provides, at the time of the study and to the best of our knowledge and belief, the most comprehensive conceptual framework for C-SCRM in scientific literature.

In the following, we synthesise the findings of this chapter and highlight the key takeaways for the remainder of this thesis. The literature review highlighted the diversity of the research field around C-SCRM while emphasising the complexity when it comes to analysing CSC risks as presented in Section 1.1. However, research providing solutions to comprehensively manage the risks is still rare and the application of frameworks remains unexplored. Summarised, the key takeaways are:

- The research around the CSC and C-SCRM is characterised by diverse and often conflicting terminologies and definitions, reflecting its infancy and complexity. This research adopts a comprehensive view, combining prior definitions to ensure clarity and cohesion.
- The literature of CSC risks reveals a complex landscape with varying interpretations of risk types, sources, vulnerabilities, and points of penetration. The understanding of these risks varies, with the human factor as a consistent, significant vulnerability and a general growing concern for cascading effects. However, current inconsistencies in terminology and interpretation hinder a unified approach, emphasising the need for standardised C-SCRM to address these risks.
- Scientific and industry research provides different solutions to address CSC risks. The early initiatives primarily mapped existing standards, but over time a focus emerged on comprehensive frameworks, specific methods, and organisational best practices, with a noted research emphasis on preventive measures over post-attack strategies. These solutions are characterised by different scopes and inputs/outputs, and their effectiveness largely remains unexplored.
- Organisations and research face intertwined challenges within C-SCRM, stemming from internal organisational misalignments, the inherent complexities of SCs, lack of standardisation, limited research depth, and the unique vulnerabilities presented by SMEs in the SC ecosystem.
- There are several structural elements and drivers originating from cybersecurity and SC theory that might impact the implementation and operation of C-SCRM, ultimately aiming to achieve an optimal balance between robustness, resilience and assurance.

3 | Interview Method

This chapter introduces the methodology of using semi-structured interviews to explore and further investigate the identified concepts in detail. The chapter is structured as follows: In Section 3.1 we explain the methodological choice as well as the overall setup of the interviews. In Section 3.2 we showcase the process of conducting the interviews as well as their analysis. Finally, in Section 3.3 ethical considerations related to semi-structured interviews are explained.

3.1 Semi-structured Interviews

The work of multiple scholars, used to build the research design for this study, identify semi-structured interviews as a useful and effective method for exploratory research using grounded theory (Makri & Neely, 2021; Corbin & Strauss, 1990; Saunders et al., 2019a). Saunders et al. (2019a) describe some benefits of semi-structured interviews, which also for this research. Within the scope of this study, the data collection is expected to encompass sensitive information concerning internal security mechanisms, as well as interactions with strategic partners and suppliers of the organisations involved. Therefore, adopting a transparent and direct approach through (virtual) face-to-face interviews is considered the most appropriate method for establishing trust with the participants and encouraging their willingness to engage in the research. Conducting interviews in person allows for a more precise exploration of the participants' roles and facilitates the provision of necessary contextual information regarding complex concepts. Semi-structured interviews, in particular, offer the advantage of posing follow-up questions to gain a deeper understanding of specific perspectives and opinions, as well as to further investigate responses and build upon previous answers. Furthermore, the interview provides participants with the opportunity to derive personal benefits and make valuable contributions to their ongoing work.

The purpose of the interviews conducted in this study is to examine the practical application of the concepts defined in Section 2.7. The focus lies on assessing their feasibility and implementation within organisations, as well as gathering participants' opinions on the relevance and interrelationships of these concepts in the context of C-SCRM.

3.2 Data Collection and Analysis

The following provides an overview of the complete interview process, from the participant's choice to the final analysis of the interviews.

3.2.1 Respondent Collection

Identifying the right participants is crucial to ensure the quality of the research interviews. Along with the scope of this study, only participants working for organisations in the Netherlands were contacted. It was tried to get a sample of participants from different industries to avoid biased information based on the sector.

Thus, also consultants/ contractors and research institutions were included to generate a holistic picture of the interdisciplinary subject of the study. Further, emphasis was put on interviewing experienced senior participants that had gained enough experience in the domain. A comprehensive list of the final participants can be found in Table IX. A total of 18 interview invitations have been sent, of which 10 were conducted. The number of 10 interviews (55% acceptance) was found to be appropriate for the scope and time of this study and delivered sufficient high-quality data. The column *Experience* indicated the participant's years experience in the current and/or related roles. In the pilot interview phase (read more in Subsection 3.2.2), it became evident that the optimal outcomes of this study would heavily rely on expertise in cybersecurity and the implementation of security programs. Consequently, the selected participants primarily possess roles in the field of cybersecurity. However, in order to investigate the extent of awareness regarding the issue beyond the cybersecurity domain, two interviewees were chosen from other fields. These interviewees include a global contract manager and a SC management advisory director.

TABLE IX. Overview of the interview participants.

Alias	Sector/ Industry	Organisation Size	Function/ Role	Experience	Mode
Contract Manager	Public	>10.000	Global Contract Manager	25 years	virtual
IT Architect	Public	>10.000	Senior IT Architect	17 years	virtual
CISO Advisor	Finance	>10.000	Strategic Advisor to the CISO	23 years	in person
CISO	ICT	1.000-5.000	CISO	10 years	virtual
Program Manager	Research	1.000-5.000	Program Manager	33 years	virtual
Consultant-1	Advisory	1-10	CEO & Consultant	25 years	virtual
SCM Director	Advisory	<10.000	Director SC Management	13 years	in person
Security Architect	Advisory	<10.000	Sr. Security Architect	25 years	in person
Consultant-2	Advisory	<10.000	Sr. Manager Cybersecurity	10 years	in person
Consultant-3	Advisory	<10.000	Sr. Manager Cybersecurity	10 years	in person

3.2.2 Interview Preparation

An interview invitation was sent out to the participants including a brief description of the study as well as the scope and mode of the interviews. According to Saunders et al. (2019a) this helps to increase the credibility, validity, and reliability of the results. Hereinafter a possible time slot was coordinated. Around five days before the interview an introduction to the research interview (see Appendix B) accompanied by the informed consent form (see Appendix C) was sent out to the interviewee. The introduction consisted of a one-pager giving the participant a closer overview of the field of research as well as an indication of possible interview themes. By that, the participant is given enough time to rethink their choice of participation and carefully consider the informed consent. The participant was given the possibility to raise questions at any time.

Simultaneously an interview guide is designed and tested within multiple pilot interviews. This led to various iterations of tailoring the questions. The final interview guide can be found in Appendix D. The guide consists mainly of open and probing questions, followed by follow-up, and closed questions to specify the participants' answers if needed.

3.2.3 Conducting Interviews

The interviews for this Master's thesis were conducted between June 5th, 2023 and June 22nd, 2023 using either virtual MS Teams meetings or in-person sessions (see Table IX). The duration of the interviews varied

from 30 to 70 minutes, with one interview lasting only ten minutes. All interviews were recorded and transcribed using MS Teams. A standardised procedure was followed for each interview. Participants were warmly welcomed, and a brief introduction of both the interviewee and the researcher was provided to create a comfortable atmosphere and offer contextual information. The overall interview process, details regarding informed consent, and an explanation of the subsequent research steps were then presented to the interviewee. Enough time was given to address any questions or concerns raised by the participants. All participants provided their consent for the interviews. However, one participant declined audio and video recording, so a thought protocol was agreed upon as an alternative. The interviews began with some warm-up questions, followed by in-depth core questions, and concluded with closing questions. Given the complexity of the subject matter and the diverse expertise of the participants, not all questions were posed to every individual. The interview sessions were customised based on each participant's background and the overall progression of the conversation. The interviews were conducted conversationally, allowing the interviewees the freedom to contribute additional information or ask questions as they desired. This approach received highly positive feedback from the participants.

3.2.4 Analysing Interviews

Transcriptions of all the interviews were made, including the corresponding timestamps. The participants further could review the transcripts for approval, if desired. The transcripts can be made available on request. The transcriptions were then subjected to analysis using the three-stage grounded analysis method developed by Corbin and Strauss (1990). This analytical approach involved open coding, axial coding, and selective coding, followed by the creation of a final theory. To facilitate and visualise this process, the qualitative data analysis software *Atlas.ti* was used. The three steps were practically executed iteratively. However, for each step, an excerpt of the code book is captured to show the progress throughout the stages in Appendix E. The analysis follows a mixed inductive and deductive approach. The whole process is oriented on the groups and constructs from the developed conceptual framework while remaining open to exploring new concepts. The following will briefly explain the coding iterations and descriptive results.

Open Coding

Open coding is an interpretive procedure used to analytically break down the data. Its objective is to provide the analyst with fresh perspectives by challenging conventional ways of thinking or interpreting the phenomena evident in the data (Corbin & Strauss, 1990). To facilitate that the interview transcripts were analysed and important statements were highlighted as quotations and assigned with a code. The step aimed to maintain an open view and code precisely. This resulted in a total of 99 codes with a total of 429 quotations. The codes had a maximum groundedness (number of quotations assigned per code) of 17 and a minimum of 1. The codebook can be found in Table A2.

Axial Coding

Axial coding involves establishing relationships between categories and their respective sub-categories. Additionally, it involves the ongoing development of categories while continuously searching for evidence and indicators associated with them (Corbin & Strauss, 1990). Several codes could already be assigned to category codes from the identified concepts within the conceptual framework. Next to that redundant codes and codes with a low groundedness were merged where possible. This led to 72 codes with a total of 425

quotations. The codes have a maximum groundedness of 20 and a minimum of 2. The results of the axial coding can be found in Table A3.

Selective Coding

Within the final stage of coding poorly developed categories are identified and checked for their conceptual density (Corbin & Strauss, 1990). All quotations included within the codes were carefully examined and reevaluated in terms of their connections and categorisation. Additionally, the category codes were structured into code groups according to the structure of the conceptual framework to provide a better overview. The final review of the coding resulted in 19 main (category) codes and a total of 69 codes with 416 quotations. The minimum and maximum groundedness of single (sub-) codes remained the same. The category codes show a maximum groundedness of 61 and a minimum of 14. The final codebook can be seen in Table A4. Code groups were assigned indicated by the name in angle brackets behind the category code.

To offer a comprehensive summary of the descriptive coding outcomes, a document-code analysis is presented in Table X. The table is limited to code groups or independent category codes, to provide a better overview. The total number of quotations may appear higher due to certain quotations being associated with multiple codes.

TABLE X. Overview of the Code-Document Analysis.

	Contract Mngr.	IT Architect	CISO Advisor	CISO	Program Mngr.	Consultant-1	Director SCM	Security Architect	Consultant-2	Consultant-3	Totals
Collaboration	2	1	9	6	8	6	1	6	6	8	**53**
CS Investments	0	1	3	1	0	2	1	1	1	4	**14**
CSC Infrastructure	1	1	9	3	1	3	1	7	0	4	**30**
Mandates	8	8	5	17	0	5	1	8	2	7	**61**
SC Cyber Assruance	0	1	5	7	1	8	0	4	0	1	**27**
SC Cyber Res./Rob.	0	0	4	0	0	0	0	0	0	0	**4**
Standards/ Frameworks	1	1	2	1	2	2	0	5	0	1	**15**
C-SCRM Objectives	0	0	2	0	0	2	0	0	0	0	**4**
Organisational Agility	3	1	5	8	0	3	3	6	0	4	**33**
Organisational Capacity	2	4	6	9	4	6	3	8	1	3	**46**
Other	6	11	11	5	5	18	5	6	3	9	**79**
SC Partner Ecosystem	15	12	2	9	7	9	12	5	3	3	**77**
Totals	**38**	**41**	**63**	**66**	**28**	**64**	**27**	**56**	**16**	**44**	**443**

3.3 Ethical Considerations

Ethics encompass the established norms and principles governing one's conduct in relation to the rights and well-being of individuals who are either directly involved in their work or affected by it (Saunders et al., 2019c). This study follows a number of ethical principles, derived from Saunders et al. (2019c), which are explained below.

Voluntary Participation

All possible identified participants were sent a formal interview invitation, leaving enough time for a decision to answer and indicate their willingness to participate. In case of no reaction or refusal of the invitation, the participant was not further harassed to participate. The invitation included a description of the scope of the study as well as the interview, which was not altered or extended at any moment. The participants were allowed to withdraw or modify participation at any time before, during or after the interview without

providing any reason. The researchers make sure to communicate and ensure that participants only share data or answer questions they are willing to.

Informed Consent

The interviews were undertaken while ensuring informed consent of all participants. This includes the provision of sufficient information, multiple opportunities to ask questions and enough time to be able to take a fully informed and freely given decision about participating in the research. This is done using an informed consent form, which was sent to the participant a reasonable time in advance of the interview. The form was further discussed together with the participant in the interview session to clarify any open questions.

Anonymity, Confidentiality and Data Protection

The anonymity of the participants is ensured throughout the whole research process. Interview transcripts as well as the final thesis document do not contain any form of personal information, by that, it is somehow possible to draw back to the identity of the interview participants. Participants' names are changed to an Alias and any information about other people or organisations is anonymised or left out. The same is applied to any confidential information that was provided during the interviews. The participants were further given the opportunity to review the transcript for approval. The original recordings are stored at a designated and additionally protected location, separated from other interview data (i. e. transcripts).

Safety and Harm

No specific safety risks were identified prior to the research. The well-being and security of the participants and the researchers are prioritised at all stages of the research process. This is achieved through implementing the above-mentioned measures, coupled with a commitment to transparency, constant communication, and responsiveness to any concerns or issues that may arise.

4 | Results

In this chapter, we present the outcomes of the grounded analysis of the interviews. The chapter is divided into three main sections. In Section 4.1 we present an overview of the participants' perspectives on the problem to establish contextual understanding. In Section 4.2 er present the results concerning the concepts developed within the conceptual. Lastly, in Section 4.3 we use the results to revise the conceptual framework and reflect on its composition as well as the established relationships. The interview participants are represented using an alias, indicated in Table IX. After each section, we provide a summary that incorporates selected quotes from the interviews, effectively illustrating the main outcomes derived from the examined concepts. The column between the codes indicates how the two statements relate to each other in their context. A legend is presented in Table XI. Additionally, the key takeaways are highlighted in a separate subsection.

TABLE XI. Legend of the symbols used in the presentation of the results.

Symbol	Indication
◯	Neutral. The quotes do not indicate any difference or do not relate to each other.
⇈	The quotes amplify each other and the context of the results.
⇄	The quotes contradict each other and underline the opposing results.

4.1 Problem Context

To set the stage for placing the results in the contextual setting of the study, this chapter presents the participants' general perspective and awareness of the problem as well as an outline of current efforts reported within the interviews. The section concludes with an outline of currently experienced challenges in implementing C-SCRM practically. This section is meant to provide an overview and detailed information on certain aspects is provided within the results in Section 4.2.

4.1.1 Supply Chain Definition & Perspectives

Organisations and functions within have different views and understandings of the (cyber) SC. Therefore, the interviews also aimed to establish an overview of the different perspectives.

Overall, participants were able to establish a holistic view of the SC, recognising that it encompasses the entire lifecycle of a product or service. This includes processes such as sourcing materials from the mine to the final product in the case of hardware, or the full contract lifecycle including supplier selection in the case of a service. Essentially, the SC is perceived as the movement of goods or components. Additionally, several interviews emphasised the significance of the CSC, particularly in industries like finance where it is regarded

as the primary SC. The Security Architect highlighted the presence of different types of suppliers (IT, OT, non-IT) within the SC, all contributing to information exchange and consequently exposed to potential cyber risks. Here the relevance emerges from suppliers or chains that have access to company information or their infrastructure. Differences are found in which supply chains are a priority to organisations. The company of the interviewed CISO e.g. prioritises the downstream (customer) SC as they become an integral part of it through their services. Especially for large organisations "internal" SCs, meaning within subsidiaries are of interest. In general, the importance of safeguarding both, the "physical" as well as the CSC is highlighted.

4.1.2 Problem Awareness & Complexity

Based on the interviews conducted, it has become evident that cyber departments of organisations in the Netherlands possess a general understanding of the imperative need to safeguard their CSC. Consultant-1 specifically highlighted this as one of the current most difficult challenges within the discipline of information security, having emerged within the past two to three years. Multiple participants pointed out that the core of the issue lies in a fundamental flaw in risk awareness. Organisations mistakenly believe that by procuring a system or service, they automatically transfer the associated cyber risks to the subsequent supplier, without fully comprehending the interdependencies within a worst-case scenario. The Contract Manager described this phenomenon by referring to procurement departments and decision-makers as *"consumers in their thinking."* However, awareness regarding these risks is gradually increasing, thanks to high-profile SC attacks that have captured board-level attention. The widespread impact of attacks like NotPetya has raised the crucial question: *"Could this happen to us?"* and has transformed it into a tangible risk. However, Consultant-3 explains, that the implications of those risks are not fully understood in some environments and are thus still not prioritised for mitigation. The CISO Advisor reports a generally high awareness within the financial sector due to the presence of various sector regulations. Additionally, the SCM Director adds that cyber risks are not a central matter of discussion within non-cyber departments e.g. SC management or operations. Contrary, the Program Manager highlights that cybersecurity displays just one perspective and not the only one that matters. Thus, to get a grip on the problem it is important to balance the interest between the different stakeholders.

The complexity of the problem is consistently emphasised by nearly all interviewees. The CISO describes C-SCRM as *"one of the hardest topics in security"* and emphasises that *"it's very hard to implement proper security in there."* The complexity and associated effort are stated as one of the main reasons, while only a few organisations started to improve their CSC security. In this context, Consultant-3 refers to the sheer amount of suppliers an organisation has to deal with as well as the complexity of being involved in different upstream and downstream SCs. As indicated in Subsection 4.1.1, narrowing the focus of discussions to specific aspects of the problem is often necessary.

4.1.3 Current Efforts & Mitigation Strategies

Although general awareness is rising, the participants see limited progress in coordinated C-SCRM efforts. Most of the efforts include specific risk assessments on a product or supplier resulting in the inclusion of some contractual clauses with security requirements based on e.g. ISO 27001. The vision and enforcement gradually decrease with the levels of sub-suppliers or contractors. However, it also became evident that some organisations, mostly larger ones, are starting to approach more comprehensive C-SCRM programs. This includes the establishment of formal functions or departments with dedicated staff, sometimes even as

a new entity. One participant reported the establishment of a dedicated department with 25 FTEs over a period of two years. The Consultant described that organisations are mainly facing the question of either developing the required knowledge decentralised or group resources for a separate function. Most of these reported programs are still in their test phase where organisations try to determine a suitable scope and needed resources within a smaller set of suppliers.

Next to the current efforts regarding a formal C-SCRM implementation in organisations, the participants highlighted some specific mitigation strategies that are either already used or emphasised for successful C-SCRM. In general, participants generally mention that organisations should carefully focus on supplier selection by only acquiring products and services that match their security expectations and shorten the SC where possible by e.g. making specific arrangements with the supplier. From a contractual perspective, it is recommended to promote the use of Experience-Level-Agreements (XLAs) instead of classic Service-Level-Agreements (SLAs) as they fail to represent the overall end-to-end experience of the product or service. On the technical side, the Contract Manager as well as the IT Architect mentioned the use of TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) as an important mitigation measure for protecting against data theft through the interception of electromagnetic radiation. Overall soft- and hardware integrity testing in-house or by an independent third party as well as a general quarantine approach for new components in the IT architecture is mentioned to increase overall security.

4.1.4 Challenges in C-SCRM

The interviews revealed several present challenges in establishing a successful C-SCRM. These challenges include the integration of SC cybersecurity into risk management and the establishment of the necessary governance structures, which is resource-intensive and particularly challenging for smaller organisations. Additionally, difficulties arise in obtaining commitment and cooperation from both security and business personnel, with still insufficient risk awareness and mitigation efforts. The sheer amount of effort required, coupled with the volume of reviewing outstanding contracts, often hinders progress in addressing SC cyber risks and contributes to the problem being ignored and pushed ahead. Staffing limitations and the lack of a comprehensive overview of the IT architecture with assets and data flow further impede C-SCRM implementation. Visibility into the entire SC is a recurring problem, alongside the challenge of executing assessments and monitoring changes in supplier posture over time. These challenges highlight the need for dedicated efforts and resources to overcome the complexities associated with C-SCRM.

4.1.5 Summary of the Findings

This section established a common understanding of the participants' perspectives on the SC as well as their experiences with C-SCRM efforts and corresponding challenges. Summarised the awareness level in IT functions is rising and organisations do have a general understanding of the issue. However, successful C-SCRM implementations are rare and mainly feasible only for larger organisations. A number of challenges regarding missing resources and the ongoing issue of achieving visibility of the entire SC became clear. Finally, a set of organisational and technical mitigation strategies are mentioned, which are perceived as being effective to increase the level of cyber SC security. Table XII summarises the subsections with selected quotes from the interviews.

TABLE XII. Summary of the problem context.

Theme	Quote #1		Quote #2
Supply Chain Definition & Perspective	*"From the mine where the silver is dug up till the end user who has the laptop in hand." (IT Architect)*	*O*	*"When you look at the supply chain for a bank, the supply chain is mainly IT. So, our focus is really on IT supply chains rather than physical ones." (CISO Advisor)*
Problem Awareness	*"This now is a new painful dossier that sort of popped up like two or three years ago. It gains traction as in we've got an issue here and then most of the organisations [have] become aware." (Consultant-1)*	⇄	*"They're more concerned about okay security of supply in that sense, do I still have all my raw materials in the future, and do I have the right transparency into my supply chain? Can I control my costs?" (SCM Director)*
Problem Complexity	*"But only few organisations actually started improving. The main reason for that is to really improve your supply chain security it's a hell of a lot of work." (Consultant-1)*	⇈	*"I think of course it gets more complex for some clients because they are also part of the downstream layer of another company's supply chain. [...] So, if I talk about supply chain risk management and supply chain security, then the complexities that I see come from getting visibility into what the organisations upstream from them are doing." (Consultant-3)*
Current Efforts	*"We now have an outsourcing office, and the outsourcing office is a formal function in the organisation where they [...] maintain all the contractor relationships with all the vendors. Even internally." (CISO Advisor)*	⇄	*"I really doubt whether they put an effort in the chain part of [cyber] supply chain [risk] management. They will eventually end up with a contract with their own supplier that may or may not contain a clause that the supplier has to manage his sub-contractors [...] etc. But that's probably where it sorts of ends like a paper clause." (Consultant-1)*
Challenges	*"The integration of supply chain cybersecurity into risk management to establish the necessary governance structures is often too resource intense for many, especially smaller organisations." (Program Manager)*	⇈	*"It's already a problem to get an overview of what are our main assets and the complete composition of it. So that's one of the processes where there's a lot of focus in the organisation to get an overview and the states of the IT assets, [...] all the data flows for IT and OT." (IT Architect)*

4.2 Exploring Concepts

In this section the interview results regarding the exploration of the in Section 2.7 defined concepts are presented.

4.2.1 Main Outcomes

Among the three desired main outcomes of SC Cyber Robustness, Resilience, and Assurance, the interviews primarily focused on the aspect of assurance. The subsequent section presents the findings related to these aspects.

SC Cyber Robustness & Resilience

The topics of robustness and resilience were only extensively discussed with a limited number of participants. The interviews revealed that robustness was commonly associated with the expected outcome of implementing cybersecurity measures. On the other hand, resilience received as much emphasis, and Consultant-1 highlighted the significance of business continuity management, disaster recovery, and crisis management capabilities for the SC. Another participant, the CISO Advisor, regarded both robustness and resilience as equally important. Additionally, the CISO Advisor differentiated resilience into two perspectives. The first focused on an organisation's ability to maintain operations, while the second perspective emphasised managing supplier relationships and having an exit plan in place.

SC Cyber Assurance

Multiple aspects regarding SC Cyber Assurance were mentioned by the participants. First of all, there are different parties and stakeholders involved in different assurance practices. The interviews revealed a consensus among the participants regarding the need for assurance and continuous monitoring initiatives to assess SC cybersecurity. The CISO Advisor expressed belief in the future reliance on such assessments, emphasising their superiority in addressing cybersecurity issues. They emphasised the importance of establishing a base level of maturity, as organisations could then focus on addressing specific areas that fall outside this baseline. Similarly, the CISO highlighted the search for a global standard or attestation that would signify a high level of cybersecurity readiness, making it easier for businesses to engage with trusted partners. Additionally, both participants stressed the need for more legislation and golden standards that define supplier obligations and provide clarity on essential cybersecurity questions. The interviews collectively underscored the demand for a standardised set of requirements governing SC cybersecurity.

The most frequently mentioned attestations are the ISO/IEC 27001 as well as SOC1 or SOC2 by the AICPA as well as the ISAE 3402 by the International Federation of Accountants (IFAC), which are including certain controls on supplier management. No international standard specifically for C-SCRM was mentioned. However, the Security Architect mentioned the upcoming Dutch standard called CYRA which is developed in a Dutch industry consortium and certified by the TUV Nederland. As an independent certification for digital resilience, it can also be used for C-SCRM. Serving as a growth model, it facilitates the progression of organisational digital resilience up to the standard of the ISO/IEC 27001. The Security Architect reported on an organisation within the Dutch critical infrastructure designing a C-SCRM by leveraging CYRA. The CISO circle of trust is mentioned as a committee in the Netherlands that is continuously working on establishing minimum requirements and assurance approaches for SC cybersecurity. Public organisations in the Netherlands make use of their own standards in the context of SC cybersecurity like the BIO (based on ISO/IEC 27001/27002) or the Algemene Beveiligingseisen Defensieopdrachten (ABDO) for defence contracts. The latter is certified and controlled by the Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Moreover, larger organisations often rely on third-party security ratings. Consultant-1 recommends, whenever possible, establishing direct personal contact to discuss security requirements with suppliers.

However, the interviews uncovered several challenges regarding the assurance of C-SCRM. Participants highlighted the varying requirements for assurance depending on the type of business, making it difficult to align expectations. The value of third-party attestations, such as SOC1 ISAE 3402 and ISMS certificates, was questioned as customers continued to demand additional detailed information. The CISO expresses criticism regarding the overwhelming number of questionnaires his organisation receives and emphasises the significant effort required to respond to them. Furthermore, he raises doubts about the effectiveness of these questionnaires, as the requesting parties rarely verify the provided answers. Concerns were raised about the adequacy of current standards, with ISO 27001 seen as providing a baseline but lacking assurance on the effectiveness of controls. Consultant-1 states: *"I think ISO 27001 is a guarantee that some attention was paid to get information security in order. But that's about where it ends. It doesn't provide any assurance on real security, [...] whether these controls are effective."* The quality of assessments, such as ISAE 3402 reports, was found to vary, casting doubt on their reliability as well as the missing scope regarding C-SCRM. Cost-effectiveness and continuous assurance emerged as ongoing challenges, with participants questioning the value and feasibility of obtaining SOC reports on an annual basis, especially for smaller organisations. Additionally, the quality of certifying auditors was called into question.

Table XIII summarises the subsections above with selected quotes from the interviews.

TABLE XIII. Summary of the main outcomes.

Theme	Quote #1		Quote #2
SC Cyber Robustness & Resilience	*"Both are equally important. They both have different perspectives." (CISO Advisor)*	↑↑	*"[The classical security objectives] need to be extended with business continuity management, disaster recovery and some basic agreement on crisis management, communication, relations, etc." (Consultant-1)*
SC Cyber Assurance	*"I'm really searching for a global standard that says if you have this attestation then you are up to par for 95% of the businesses that can do any business with you" (CISO)*	↑↑	*"They said you need to be certified, either ISO 20000 or ISO 27001 but in the statement of applicability it doesn't say anything about this program's [C-SCRM] scope. So it's a scoping discussion, isn't it? It's not really an insurance because you do it once a year. And there are a lot of things that are changing. So you need to have insurance on a more continuous basis." (Security Architect)*

4.2.2 Structural Elements

The structural elements were discussed frequently with a total of 107 quotations in 16 codes. Especially the ecosystem perspective received much support.

CSC Infrastructure

Organisations typically take a collaborative approach, involving both business and IT/OT departments, to comprehensively analyse their SCs. Participants acknowledge that the development from monolithic systems to now fully automated and integrated systems has resulted in a significant increase in the attack surface, making it more challenging to get a comprehensive overview of the underlying architecture and its dependencies. A major challenge is to understand what a supplier specifically provides to an organisation and to be able to assess the corresponding risks. Organisations typically start by focusing on the most critical business processes and then drill down to the composition of their IT and OT environments, including the inventory of cyber assets and data flows and thus, corresponding suppliers. However, Consultant-3 noted that companies often struggle to understand the security implications of these relationships.

The interviews have shown that for successful C-SCRM it is important to consider both, the business risks as well as technical risks and evaluate a supplier's criticality based on that. The participants underlined the criticality of supplier evaluation in the context of their contribution to business processes, associated risk levels, and the nature of their involvement. The Contract Manager asserts the need to determine the crucial role of suppliers within the organisation's operational workflow and from that determine how to treat the relationship. A tier-based evaluation system or classification scheme, described by the CISO Advisor and Security Architect, further enhances this understanding by categorising suppliers according to their significance, ranging from strategic partnerships to functional roles. The consensus from a regulatory viewpoint in the financial sector focuses on the necessity of prioritising vital clients and core functions during supplier evaluations. This perspective is complemented by Consultant-1's emphasis on risk assessment, which advocates for maintaining flexibility while mitigating high-risk partnerships. On the other hand, the participants placed equal importance on considering the technical criticality of suppliers. Hereby, the network expansion through the acquiring of external products/ services, how they are attached to the organisation's surface, specifically the type of connection as well as the access to systems and infrastructure plays a vital

role. The CISO names examples for critical systems like mail systems, CRM systems or data storage. Furthermore, OT components tend to demand much more specific risk assessments considering dependencies to other components while the business risk here is more obvious in case of a disruption. Overall, depth seems to depend on the sector and used technology parts.

A specific but noteworthy case is mentioned by the CISO Advisor around securing financial flows. Therefore transaction flows have to be managed carefully regarding the complex underlying infrastructure that is unique to this sector. Due to the high interconnectedness of international systems like SWIFT, possible disruption or breaches may risk billions. These dependencies pose immense challenges to the whole financial industry.

SC Partner Ecosystem

All participants acknowledged the transformation from the classical SC towards the development of a complete ecosystem around today's organisation, representing the network that has to be included in security considerations. Those ecosystems represent dependencies. The SCM Director names ASML as an example organisation that heavily depends on its ecosystem to create the majority of its outputs. The CISO Advisor highlights the different types of third-party products and services that all demand different mitigation measures. A general overview of this ecosystem is essential. Additionally, the Program Manager emphasises the role of system integrators in ecosystems that significantly impact security and are often not carefully considered. The remainder of this section will more precisely elaborate on the relevance and specific aspects of alignment, relationships, and responsibilities for C-SCRM within those ecosystems and single organisations.

As briefly mentioned in the previous sections, aligning the different perspectives is crucial for successful C-SCRM. Therefore, internal alignment is seen as an important factor by all participants. However, the Program Manager notes that the different perspectives within organisations are often not well aligned. The Contract Manager highlights the challenge of aligning the mindset of business decision-makers with the security requirements of services, emphasising the growing importance of decision-makers being knowledgeable about security standards like ISO 27001 certifications. It is added that strategic and global aspects of e.g. contract management are often handled separately from operational details. This is further emphasised by Consultant-1 who points out the difficulties faced in internal alignment, where responsibilities may be shifted to other departments, and decision-makers may lack understanding about what to ask for, and discuss with certain stakeholders. Thus, participants perceive the general need for more improvement in terms of internal alignment. Most of the participants also acknowledge the interdisciplinarity of the topic ranging from IT to HR departments describing it as an eye-opener for organisations and the SCM Director adds that risk assessments in this context *"should be cross-functional by definition"*. Participants also pointed out that product acquisition decisions are now made by an internal interdisciplinary team. The same development is seen by some participants for external alignment. While the SCM Director highlights the need for digital connectivity and real-time alignment between partners in physical SCs, the Program Manager highlights the importance of aligning processes and establishing incident handling capabilities and information sharing as crucial factors in C-SCRM also indicating that those capabilities should be prioritised over gaining visibility into every detail of the SC. This is complemented by the Cybersecurity Architect who acknowledges the significance of external alignment in cases where suppliers have access to the main infrastructure and sensitive information. Both dimensions of alignment are closely related to the careful definition of responsibilities, both internally and with SC partners. Multiple participants highlight the importance of shared responsibility for security, both within the SC and internally, and advocate increased accountability at the executive

level. The IT Architect emphasises a delegation of security measures between the partners and Consultant-1 emphasises the need to make contract owners accountable for certain parts of security within the contract lifecycle.

The interviews highlighted the importance of considering the diverse nature of supplier relationships in C-SCRM. Suppliers can range from large, strategic partners such as Microsoft and IBM to smaller, critical suppliers. The CISO highlights the difficulty of assessing a supplier's security posture in relationships where partners only share certain points of connection and Consultant-3 also questions whether organisations allow partners to take a detailed look at their IT infrastructure. It has become clear that the influence on large strategic partners like Microsoft is restricted, and companies have to trust their reputation. The IT Architect as well as the SCM Director emphasise the dimension of power in relationships. Therefore, suppliers are aware of the consequences of failing to meet their customers' security requirements. In a sensitive environment that can lead to potential damage to the suppliers' reputation as well as the risk of losing current and future customers. The SCM Director adds that the dominant player within an ecosystem is usually in a position to issue mandates. Participants report some common issues that are present within SC relationships. Challenges faced by local decision-makers include building strong relationships with suppliers, as well as distinguishing between the roles of supplier and partner. Another problem arises from the short duration of most contracts, limiting the ability to develop long-term partnerships. Additionally, the SCM Director adds that finding a balance between efficiency and resilience in the SC is proving to be a difficult task, as it requires managing costs while ensuring robustness against disruptions.

However, a number of measures to improve relationships are identified by the participants. The Contract Manager highlights that maintaining longer-term contracts fosters investment and commitment from both parties, leading to mutual benefits and a more comfortable relationship. Long-term partnerships create a different kind of relationship that allows for greater trust and collaboration. The IT Architect highlights that building trust is crucial, and attending partner conventions and openly acknowledging suppliers' reliability helps establish them as trustworthy partners. Cooperation and partnership should go beyond contractual obligations and involve suppliers in activities such as research and development. Additionally, proactive support can be provided to smaller vendors, assisting them in enhancing their security measures. These results enhance communication, trust, and joint efforts, contributing to improved C-SCRM, while the latter is elaborated on in Section 4.2.4.

As described above, the interviews revealed that trust and transparency are particularly important in supplier relationships. Trust is crucial, as it is challenging to verify every supplier's operations, but cherry-picking and thoroughly evaluating a few key suppliers can mitigate risks and raise awareness on the supplier side. The IT Architect recognises that an organisation cannot achieve complete control over an entire SC. Establishing trust enables effective collaboration and investigation when incidents occur, relying on the professionalism and integrity of suppliers. Trust is built through certifications, dialogues, strong partnerships and transparent processes that promote open communication and shared responsibility. Transparency is valued as it fosters better understanding, timely information sharing, and proactive measures in response to incidents. By promoting trust and transparency, SC participants can strengthen their relationships and collectively address challenges in the SC Partner Ecosystem.

Table XIV presents a summary of the concepts mentioned before.

TABLE XIV. Summary of the structural elements.

Theme	Quote #1		Quote #2
Architectural Overview	*"Most organisations try to analyse their own SC and have a process for that. Most bring people from the business department as well as IT/OT department together for that." (Program Manager)*	⇄	*"It's already a problem to get an overview of what are our main assets and the complete composition of it. Even if you ask an IT guy [...], do you have an overview of the complete CMDB? Forget it." (Security Architect)*
Supplier Criticality	*"We first look at the business function that should be fulfilled. So, if it's part of the core [...] functions, then it is more important for [...] [us] than if it's something like facility management or a supporting function.." (CISO Advisor)*	⇈	*"We classify all the suppliers from A-Z [...]. Everything that's A to D has some way of access to our systems, access to our infrastructure, and direct access to customer data." (CISO)*
Alignment	*"The internal alignment has to be improved in most organisations e.g. when the contract department struggles to derive the cyber requirements. It's about aligning the different internal perspectives towards the problem." (Program Manager)*	⇄	*"That is the hardest part because very often the business will point to the procurement department saying that's what you're doing." (Consultant-1)*
Relationships	*"They can have an incident they can even have a huge incident but if they did everything to prevent it and they are very open about what happened and they help us if it also impacted us, helping us through recovery, why shouldn't they become our best supplier ever?" (CISO)*	*O*	*"So, the problem is that most of the contracts are for two years. What kind of partnership can you build in two years? Nothing." (Contract Manager)*
Supplier Size	*"They have to trust the certificates and the blue eyes of the vendors. That belongs to accepting some certain uncertainty." (Cybersecurity Architect)*	*O*	*"Unfortunately in this day and age doing business requires you to do cyber. So, if you can't make your business model work, including security, then I don't think you deserve a seat at the table." (Consultant-2)*

4.2.3 Mediating Elements

Within the mediating elements Mandates as well as standards and frameworks were heavily discussed concepts. But also C-SCRM Objectives, as well as Cybersecurity Investments, brought up some interesting results. This resulted in a total of 94 quotations in 14 codes.

C-SCRM Objectives

The theoretical details of C-SCRM Objectives were only discussed with two participants. As already mentioned in Section 4.2.1, there is a general understanding that the classical CIA-triad will remain as the core of information security but has to be extended with business continuity, disaster recovery, and crisis management objectives. The CISO Advisor mentioned resilience and privacy as perspectives where the CIA-triad has to be extended. However, no specific suggestions were made and the complexity of properly handling and framing those objectives was highlighted. Additionally, Consultant-1 mentions that the ISO 27001 standard has lacked clarity in its last three iterations, particularly regarding its extension towards resilience.

Cybersecurity Investments

The majority of the participants do not observe coordinated cybersecurity investments within the SC ecosystem. Multiple participants expressed scepticism about the current awareness and adoption of holistic approaches but acknowledged it as a useful measure. The reasons mentioned are the high complexity of cybersecurity investments as well as the lack of commitment and high coordination efforts, especially when multiple supplier levels (sub-suppliers) are included. However, some initiatives are already in place. Consultant-3 highlights long-term contractual relationships as a committed investment to foster partnerships in a SC. The IT Architect emphasises incident-driven investments, relying on their supplier's partnership and shared

investigation capabilities when security compromises occur. The CISO Advisor as well as Consultant-3 highlight shared investments on the industry level e.g. in innovation committees with partners and suppliers or the development of shared response services. As part of the establishment of a C-SCRM, the Security Architect describes an ongoing initiative focused on exploring opportunities for developing a shared SOC with strategic suppliers in the future.

Mandates

The concept of mandates was found to be manifold. The key findings encompass the ways organisations establish requirements for their suppliers and how they effectively manage these expectations. Additionally, the results shed light on the significance of forthcoming regulations.

The most frequently mentioned measure of organisations was the creation of customised lists of requirements for suppliers, often based on excerpts of controls from established standards like ISO 27001 or NIST CSF. Additionally, the demand for a respective certification often poses the basic requirement, further extended by questionnaires. These may vary depending on the type of acquired service product but are also often used as a set of minimum requirements independent of the supplier. Criticism of this approach was presented in Section 4.2.1. In summary, it addressed the decreasing value of independent attestations and missing verification of those requirements. This criticism is partly confirmed by some participants. The Contract Manager points out that there are currently no KPIs in place to monitor contractual requirements, although a re-assessment of the suppliers' posture is done yearly. Furthermore, the Security Architect states: *"We don't believe only your ISO certificate but want you to proof, show me, tell me, prove me."* Contrary to that, the participants mentioned different ways of verifying their requirements. The IT Architect emphasises a mixed approach of physically checking certain requirements and using detailed checks for specific hardware parts. The Security Architect and Consultant-3 highlight the importance of ensuring the right to audit. Especially existing contracts as well as the inclusion of sup-suppliers pose hurdles to ensuring the right to audit. The CISO describes an individual approach per supplier in conducting conversations about findings and outcomes of the attestations as well as how they will address those findings in the future. Some further more general approaches are highlighted by the participants. Both the Contract Manager and Security architect point out that requirements and associated assessments should already be carried out in the contract management phase. As described before it is deemed as important to ensure that (certification) requirements also apply for sub-contractors or sub-suppliers where possible. Consultant-3 also describes the observations of requiring suppliers to ensure redundancy in their suppliers and that organisations pull their negotiation power together to lay down mandates on certain suppliers. A second aim was to explore the ways suppliers deal with the increased amount of requirements. Hereby, differences emerge from the interviews. The Contract Manager reports of suppliers that still question the necessity of cybersecurity requirements while other participants highlight that by now, almost all suppliers understand that cybersecurity has become a main requirement in supplier relationships. However, Consultant-1 describes that elaborate discussion and explanation are needed on detailed requirements and not many suppliers appropriately implement measures. Participants from sectors subject to stricter regulations demonstrate greater awareness and acceptance of cybersecurity requirements. According to the Security Architect, when requirements are discussed openly and collaboratively, suppliers demonstrate a commitment to enhancing their security posture and learning from larger partners in response to the growing demand for these requirements.

Another perspective on mandates is the current landscape of external regulation, especially considering the

upcoming EU regulations with e.g. NIS2 and CRA, which was discussed with almost all participants. Similar to the discussion on assurance in Subsection 4.2.1, participants welcome additional regulation regarding SC cybersecurity. The CISO specifically mentions the demand for a regulation to refer to when discussing minimum requirements in a SC. Opinions on the expected effects of forthcoming EU cyber regulations varied among the participants. The IT Architect believes that vendors and resellers will be able to comply with the requirements and gain the trust of their customers, although they may not examine their SCs thoroughly. The CISO and IT Architect draw parallels with the GDPR, where companies solely expect compliance from their partners. The CISO further expresses curiosity about the level of detail required for compliance and thus the effectiveness of the regulations. Some participants hope that the regulations will bring about positive security practices, while others are sceptical, citing the weak GDPR enforcement as a reference. Overall, there was consensus that regulatory pressure would lead to incremental improvements in SC security, although it would take time to achieve comprehensive results. The NIS2 Directive and other regulations were seen as drivers of awareness and enhanced C-SCRM. Participants recognised the need for a clear understanding of SCs and the responsibility of board members in managing risks. The regulations were expected to facilitate knowledge exchange and drive action from both large companies and their suppliers. It is of interest to mention that the SCM Director, representing a perspective without any cyber background, had no awareness of the upcoming regulation.

TABLE XV. Summary of the mediating elements.

Theme	Quote #1		Quote #2
C-SCRM Objectives	*"I think the CIA triad is the core. So, I think if you really bring it back to the core of information security it is about confidentiality, integrity, and availability and I think that will hold." (CISO Advisor)*	*O*	*"They need to be extended with business continuity management, disaster recovery and some basic agreement on crisis management, communication, relations, etc." (Consultant-1)*
CS Investments	*"I haven't seen any movement in that direction yet. And I'm also having a hard time imagining it" (Consultant-1)*	⇄	*"Now we're investing with some of the strategic partners, [...] how can we collaborate and build our own SOC with the partners and perhaps with our main infrastructure provider in the future." (Cybersecurity Architect)*
Mandates: Requirements	*"We have direct questionnaires for the third parties that they have to fill in and that's more or less based on both, ISO 27000 and NIST controls. It's a list of questions that we have for them that they need to provide answers [on]." (CISO Advisor)*	⇄	*"We have a lot of customers that ask us, even though we send them our SOC1 ISAE 3402 and ISMS certificate, they still send us, a hundred plus is not an exception, questions that we have to answer [...]. Those are questions that are becoming more and more. If we keep on doing this, then what's the value of third-party attestations?" (CISO)*
Mandates: Regulation	*"It will improve bit by bit. Having some regulatory pressure on the topic doesn't hurt. It's one of these topics that doesn't fix itself. It needs a little push and I do think that SC security will improve." (Consultant-1)*	⇄	*"I first have to see if it's ever going to be effective. I don't see any open market consultations from any country. I don't see an open market consultation about NIS2 implementation in Germany, or in the Netherlands." (CISO)*
Standards & Frameworks	*"There is a need for a standardised set of requirements about supply chain cybersecurity. Therefore, focus should be on European level or sector level to prevent too many competing sets of requirements [...]. Focus on uniform and commercially interesting sets of requirements" (Program Manager)*	⇈	*"We decided we will define a policy, with some drivers and objectives and link them to ISO controls, because in security everybody's using ISO, NIST or ISF, to find a common language and common ground." (Cybersecurity Architect)*

Standards and Frameworks

The use of standards and framework in the context of C-SCRM was already partly discussed in this section as well as Subsection 4.2.1. The main frameworks mentioned are the ISO 27000 family, NIST CSF, standards of the Information Security Forum (ISF) as well as different governmental and sectorial best practices and

standards. Especially in the Netherlands, CYRA seems to be a promising initiative. However, no specific C-SCRM standard was mentioned. Among the participants, the Security Architect was the only one who was familiar with the NIST SP 800-161r1 framework, but also acknowledged the dominance of ISO standards in Europe and expressed a preference for building upon these standards. Participants highlighted that the use of standards indeed helps to establish a common understanding and use of terminology as well as assures basic security within an organisation. Contrarily, the use of generic standards poses a scoping challenge to assure real SC security as mentioned by Consultant-1 and the Cybersecurity Architect. The Program Manager emphasises the importance of standardised requirements at a European or sector level to avoid competing sets and promote effectiveness. Sector initiatives have demonstrated greater efficacy, and generic approaches should be avoided. Table XV shows a summary of the previously elaborated concepts.

4.2.4 Moderating Elements

The moderating elements were discussed comprehensively with a total of 132 quotations and 15 codes. Especially collaboration, visibility, and flexibility were subject to elaborate discussion.

Collaboration

The participants show a general consensus regarding the importance of collaboration in the context of C-SCRM and highlight several key reasons. The CISO Advisor emphasised the shared goal of defending against common adversaries (the good vs. the bad) and the belief that working together is essential in achieving this objective. Collaboration is viewed as an opportunity to share knowledge and improve defence strategies, with a focus on finding smart solutions that alleviate the workload for all involved parties. The Dutch approach, which is seen to prioritise collaboration, is regarded as highly effective for C-SCRM by the Program Manager. It is also added that collaboration facilitates the pooling of expertise and encourages compliance among a larger group of organisations. Trust is identified as a critical factor in successful collaboration, underscoring the importance of building and maintaining strong relationships. Finally, sector-wide collaboration is seen as essential for establishing a common understanding and aligning perspectives in C-SCRM efforts. To facilitate collaboration participants identified different enablers. The IT Architect as well as the Program Manager emphasise the definition of clear responsibilities and open communication as an essential factor. The Cybersecurity Architect highlights the importance of prioritising strategic value over price when selecting suppliers, as solely focusing on cost may impede supplier innovation and hinder effective collaboration, leading to increased effort and costs in the long term. Consequently, re-educating procurement personnel to avoid excessively cost-driven contracts emerges as a crucial recommendation. Finally, current and upcoming regulations are seen as an enabler, ensuring consistency, while promoting knowledge exchange and structured frameworks for collaboration. The CISO Advisor names that as a reason for the increased maturity in the financial sector.

The participants further describe different modes of collaboration that are already implemented. One approach is the formation of inter-company groups in the Netherlands, such as the CISO circle of trust, or the CIO platform, which brings together CISOs/CIOs from major companies in the Netherlands to discuss cybersecurity matters. Another mode involves collaborative initiatives within specific sectors, such as the combined SOC initiative in the financial sector including the National Cyber Security Centre. The CISO points to a similar initiative within the medical sector. The Program Manager also gave an example of collaboration in the sector of water management in the Netherlands. However, these do differ in the way

that they are not necessarily facilitating collaboration within the SC ecosystem alone and Consultant-2 adds that sector initiative poses the risk of being too isolated as threat actors do not only focus on one sector. In this context, the CISO Advisor highlights that cross-industry collaboration is also being explored, to exchange knowledge and threat intelligence across different sectors. Partnerships for cyber security innovation are another avenue for collaboration, allowing organisations to work together with innovation initiatives and sub-contractors to advance cyber security practices. The CISO reports that collaboration, specifically for smaller businesses, often involves regular meetings and information sharing between security teams, fostering relationships and building trust. Furthermore, collaborations extend to supplier involvement, including joint R&D activities, and sharing audit results and resources among organisations with shared suppliers. The Security Architect describes the mode of larger organisations leveraging their security teams to increase a supplier's security posture or even lend them security personnel for a limited time. Consultant-3 emphasises that more mature organisations often collaborate to share intelligence, and best practices, and audit their suppliers, leveraging their collective negotiating power to drive security improvements. The Cybersecurity Architect highlighted a specific collaboration initiative in which they invited a large organisation with a successful C-SCRM in place to share their experiences. This collaborative exchange aimed to gather insights and lessons learned in setting up an organisational program. In contrast, participants still describe some barriers to achieving collaboration. The Contract Manager sees challenges for collaboration in more sensitive environments. Consultant-2 highlights that the governance structures to facilitate collaboration in large SC ecosystems are missing or just not made available in terms of resources. Both participants also underline the unknown consequences and legal situation of sharing information, potentially resulting in disadvantages.

The interviews further revealed a demand for external support to facilitate C-SCRM. Participants expressed the hope that specialised market players would emerge to provide C-SCRM services, such as vendor screening and rating. Additionally, research organisations may support satisfying the need for understanding system dependencies within the SC on a sector-wide level, simultaneously raising awareness where the significance of the problem might not be fully recognised by individual organisations. It is acknowledged that substantial security knowledge is required, which may be lacking within organisations, leading to a reliance on external expertise. The role of consultants was highlighted as crucial in helping clients understand critical suppliers, assessing their exposure, and implementing innovative monitoring methods to enhance efficiency, especially for smaller organisations.

Organisational Capacity

This group includes the concepts SC Visibility, Cybersecurity Readiness, and Situational Awareness. The results are presented below.

SC Visibility

Gaining visibility into the whole SC ecosystem including multiple levels of sub-suppliers and sub-contractors is considered essential for successful C-SCRM but poses one of the greatest challenges for organisations. By now firms have limited knowledge about their suppliers and little effort is put into understanding the extended SC. Participants question the feasibility of acquiring a comprehensive picture considering the required resources. Participants describe current efforts only if required from a legal perspective (e.g. GDPR) and for several critical suppliers in a test stage. The CISO and Consultant-2 highlight that missing formal contracts and relationships with suppliers of suppliers hinder assessment and communication since firms

might be hesitant to provide granular information without a contractual basis. Consultant-3 points out that visibility efforts are limited as firms still struggle to manage their primary suppliers. Besides that, a number of measures and approaches to improve SC Visibility were discussed. The IT architect and the CISO Advisor emphasise the establishment of contractual clauses to ensure the obligation to share information about sub-contractors used and the requirements to forward certification obligations to sub-suppliers. The Cybersecurity Architect mentioned an approach of delving into sub-suppliers until reaching major service providers such as Microsoft or Amazon. Last but not least, several participants noted the trend of prominent market players acquiring their key suppliers to incorporate them within their internal ecosystem. As already mentioned in Section 4.2.2, the Program Manager emphasised prioritising the establishment of shared incident-handling and information-sharing capabilities instead of trying to achieve detailed visibility.

Cybersecurity Readiness

Cybersecurity Readiness as defined in Section 2.7 of this study was found difficult to conceptualise for the participants on a holistic level and thus only discussed briefly. Consultant-1 emphasises the importance of organisations proactively integrating C-SCRM as a fundamental component of their comprehensive security program, treating it on par with other information security risk mitigation initiatives. The Program Manager points out that in addressing C-SCRM it is important not to assume that all risks can be mitigated by securing the acquiring SC. Instead, firms should focus on defining processes to deal with incidents and establish vulnerability handling. Generating awareness and getting the board level involved through a risk-driven rather than a compliance approach is seen as a central prerequisite for successful C-SCRM. Other organisational prerequisites are comprehensive governance structures with proper assignment of responsibilities and sound risk assessments. On a technical level, the Cybersecurity Architect mentions proper documentation and management of the present architecture including service management for IT and OT as a requirement.

Situational Awareness

Sources and formal processes to stay aware of the changing posture of suppliers as well as recent vulnerabilities are still limited in the context of C-SCRM. Organisations employ various methods to stay aware of their suppliers' security posture. The IT Architect describes annual security analyses based on reports from governmental institutions within the sector of high criticality. The CISO highlights the collaboration with some governmental institutions for threat intelligence. Next to that, participants highlight further ways, inter alia, utilising external platforms, services, and rating for continuous monitoring like BitSight, subscribing to threat intelligence feeds and newsletters like *Connected2Trust* in the Netherlands, participating in Information Sharing and Analysis Centers (ISACs), and engaging in regular meetings between security teams to review reports, trends, and incidents. However, there is a need for structured monitoring of risks especially about IT and OT systems and political developments to ensure a comprehensive understanding of the supplier landscape. Overall, monitoring changes in supplier posture and ensuring the consistency of assessed posture over time to gain situational awareness are seen as crucial aspects in C-SCRM but are still seen as a challenge by some of the participants.

Organisational Agility

Organisational Agility includes the concepts SC Agility and SC Flexibility. The interviews did not result in a precise distinction between agility and flexibility. Thus, the results are presented together.

Overall flexibility is a comprehensively discussed concept, that still poses challenges on an operational level for a lot of organisations. Some participants admitted that switching suppliers in case of disruptions or incidents is practically not feasible for their organisations and if so, will require a lot of effort and a long time. Reasons for that are majorly strong dependencies e.g. in the case of long-term infrastructure providers where transferring huge amounts of data/ assets would come with an unmanageable cost and further continuity issues. The Contract Manager describes that even having a multi-vendor approach does not assure variable adjustment of capacities as other businesses might deal with the same disruptions and thus limit availability at the supplier. The CISO Advisor highlights that preparation of those scenarios is difficult and most likely has to be solved in improvisation. Additionally, in some sectors, the availability of redundant niche suppliers is limited by default. This is confirmed by Consultant-3, who points out that flexibility, as well as agility, will be very dependent on the specific product or service. The results show as well that it is generally easier to switch from smaller suppliers. Contrary, Consultant-1 sees a general development less focused on flexibility and more towards consolidation of suppliers due to cost-cutting and efficiency reasons. Consultant-3 highlights the willingness of organisations to achieve flexibility and agility, but simultaneously the restricted ability to effectively implement and execute such changes.

TABLE XVI. Summary of the moderating elements.

Theme	Quote #1		Quote #2
Collaboration	*"The next few steps you suggested as in resource sharing and close collaboration, I'm not really seeing yet." (Consultant-1)*	⇄	*"The answer is yes. And the closer we are the more. [...] So, we want to team up with our partner banks and then come up with solutions that provide an ecosystem that is solid and secure, including also partners and subcontractors. " (CISO Advisor)*
SC Visibility	*"No, no, no. We don't have visibility. Well, I can want it, but for my organisation, it's too difficult and then I said OK, it's a question for about 5 years." (Contract Manager)*	↑↑	*"It's not feasible and too resource intensive to get a grip on all the details in the supply chain also considering constant changes to it." (Program Manager)*
Cybersecurity Readiness	*"So, I don't think you should wait, but I do think you should get the supply chain in order as part of a larger security implementation covering also the other information security risks within your organisation." (Consultant-1)*	◯	*"So one of the prerequisites for this kind of programs to succeed is to be risk-driven because it's risk management, not the compliance tick in the box." (Cybersecurity Architect)*
Situational Awareness	*"That's the question of being able to monitor changes to the supplier's posture. So, the supplier, that was not critical today and was not accessing sensitive information today changes in what they are now able to access. A lot of times that slips through the cracks. I think the last thing I would say is being able to ensure that the assessed posture at the time of doing the assessment remains the same. So, monitoring of the supplier's posture [remains a challenge]" (Consultant-3)*	⇄	*"And therefore, I truly believe that this kind of assurance and continuous monitoring initiatives that are far better equipped to do this kind of assessment, are the way forward and we should have some sort of future vision where we can rely on this kind of assessment at least for a quite substantial level." (CISO Advisor)*
Organisational Agility	*"I remember one situation and that was where the preferred Supplier #1 had a DDoS attack. And we called #2 and #3, we asked them to scale up and they said sorry, we have other clients with the same problem, and they pay us more and they are in the critical infrastructure." (Contract Manager)*	↑↑	*"So yes, we have certain procedures, yes, we can in a way mitigate and move away from certain suppliers, but you're never going to merge away within a year to any other suite like Google or something, it's just not going to happen. It's a fantasy." (CISO)*

However, the interviews revealed a number of different approaches and initiatives to increase SC Flexibility and Agility. Multiple participants highlight that their organisation works with a multi-vendor approach. However, experiences with switching between suppliers in case of a disruption are rare, and limit the ability to discuss the agility aspect. The CISO Advisor distinguishes between two perspectives of flexibility and agility on an operational level, that are also driven by sectoral regulation. The first perspective emphasises

the need for an exit plan to enable the termination of supplier relationships if necessary, while the second perspective focuses on ensuring continuity through measures that support uninterrupted operations. The Cybersecurity Architect similarly describes an exit and replacement strategy, which aligns with the organisation's overarching procurement policy. Those measures are further reinforced by continuous monitoring activities about supplier alternatives by the contract department. As already mentioned in Section 4.2.4 under the concept of SC Visibility, large market players can also integrate critical suppliers into their ecosystem by acquiring the whole company. On the other hand, the SCM Director observes the general trend of collaboration to establish dynamic (physical) SCs including scenario planning which demands a high level of transparency to develop subsequent strategies together with suppliers. A summary of the findings in presented in Table XVI.

4.2.5 Summary of the Findings

In this section, the main results around the derived concepts were presented. The results highlighted the importance and fit of the three main outcomes SC Cyber Robustness, Resilience and Assurance. Especially assurance was subject to extensive discussion and the need for a common approach regarding SC cybersecurity is expressed. The Dutch initiative CYRA might pose a possible solution. The interviews again emphasised the importance of the structural elements in creating a baseline for successful C-SCRM. Especially the needed architectural overview and subsequent supplier criticality were found to be of importance. Further, understanding and dealing with the different kinds of relationships in an SC Partner Ecosystem and establishing suitable ways of aligning each other's perspectives and processes external as well as internal is crucial. Within the mediating elements, it has become clear that the classic information security objectives are also the core of C-SCRM. However, resilience aspects like business continuity and disaster recovery are just as important and have to be added. The results show that coordinated investments in cybersecurity are mainly done in the form of industry consortiums of large mature organisations. Specific coordination mechanisms are not discussed. The investigation of mandates has revealed how organisations pose customised requirements to suppliers and the use of certifications and questionnaires. The concept is closely connected to the use of standards and frameworks, where it was shown that no specific C-SCRM frameworks are being used, but rather a set of established general cybersecurity frameworks. The moderating elements have underlined the importance of collaboration within a supplier ecosystem for better security. SC Visibility is identified as one of the most important concepts which subsequently still poses the greatest challenges for organisations. The interviews revealed some prerequisites for a successful C-SCRM and highlighted the challenge of continuous monitoring of suppliers' security posture. Finally, SC Flexibility and Agility are an ongoing issue in operations.

4.3 Revision of the Conceptual Framework

Based on the presented results of the interviews, the following will reflect on the in Section 2.7 established conceptual framework. Therefore, the aim is to revise the composition as well as indicate relationships between the concepts where possible. The described changes are not meant to present a final validation of the conceptual framework but rather visualise the progress throughout the methodological steps in this study. Further interpretations of the results in detail are presented in the discussion in Chapter 5.

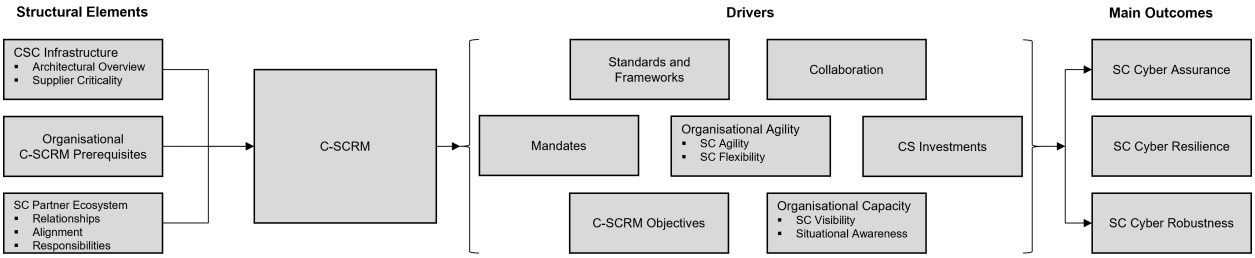

FIGURE VII. Final revised C-SCRM conceptual framework. Own illustration.

The results and insights from the interviews led to some changes in the concepts as well as their position and relation in the conceptual framework. The categorisation of the concepts into structural elements, drivers and main outcomes was found to be sufficient to indicate a vague relationship to C-SCRM. However, the distinction between mediating and moderating elements could not be sufficiently proven and has been found to lead to a narrowing of the concepts and strong contextual dependency. The theoretical classification is deemed as too rigid for a multifaceted topic like C-SCRM. Therefore, the groups are dissolved and all the drivers are presented together, without any attempt to indicate the importance or relationship between them. Furthermore, some concepts of the structural elements were renamed and added. The interviews showed that the sub-concepts of the CSC Infrastructure are experienced in a broader context in practice. Thus Architectural Overview and Supplier Criticality do represent a broader picture of how organisations approach the analysis of their CSC. As the definition and allocation of responsibilities, both internally and with suppliers, was mentioned by many participants, it was added as a sub-concept in the SC Partner Ecosystem group. The theoretical understanding of Cybersecurity Readiness was found to be less relevant in direct relation to C-SCRM. However, participants still highlighted some general prerequisites. Therefore, the concept of the Organisational C-SCRM Prerequisites was added to the structural elements. The final revision of the conceptual framework is shown in Figure VII.

5 | Discussion

The results in Chapter 4 gave a comprehensive overview of the perception and implementation of C-SCRM and the concepts identified in this research in practice. Within this section, the results in the context of the theoretical foundations of the concepts from Chapter 2 are discussed.

5.1 The Current State of C-SCRM in the Netherlands

The versatility of C-SCRM has been highlighted in the various perspectives provided by the participants of this study. The notion of the SC is understandably multifaceted, with some viewing it from a product or service perspective, while others emphasise the importance of different types of SCs and its suppliers. A key insight is the recognition of the CSC as crucial in the aspect of SC management, especially in the finance industry where it stands out as the SC with the most importance. The relevance of the downstream SC seems to take precedence for some organisations, indicating the vital role of customers and possible risk propagation. Despite the increasing awareness, a glaring issue is the insufficient understanding of the complexities of the SC and C-SCRM among organisations in the Netherlands. While businesses are aware of the need to safeguard their CSC, the issue lies in an often still faulty risk perception, especially in business functions. Many organisations operate under the mistaken belief that procuring a product or service automatically transfers the associated cyber risk to the supplier. This oversimplified view neglects the interdependencies that can potentially lead to amplified risks. However, the positive outlook is the gradual increase in risk awareness, mainly triggered by high-profile SC attacks and board level discussions, leading companies to take a more proactive stance on risk mitigation. It remains questionable whether awareness, particularly at board level, correlates with an understanding of the value and importance of securing the SC. The complexity of C-SCRM is unanimously acknowledged by all the participants, with some describing it as the most complex issue in security today and the main reason for the slow progress. The challenges experienced are manifold - ranging from the difficulty of integrating C-SCRM into the organisational risk management with the needed governance structures, the lack of defined responsibilities and the limited resources available. Despite growing awareness, there remains a gap in the successful implementation of coordinated C-SCRM efforts. These findings are in line with Section 1.1 of this study as well as the recent findings of Papaphilippou et al. (2023).

While some product/service or supplier risk assessments and classifications are carried out, resulting in contract clauses with security requirements, these measures are fragmented and often lack possibilities of enforcement on a sub-supplier/ contractor level. However, it is encouraging to observe that larger organisations are beginning to develop more comprehensive C-SCRMs, including the establishment of dedicated functions or departments. Additionally, participants described organisational and technical mitigation strategies which should be considered in this context.

5.2 Understanding the Supply Chain and its Ecosystem

The SC Partner Ecosystem signifies the increasing complexity of relationships that organisations operate in. Two main aspects that shape this ecosystem are internal and external alignment. Empirically, organisations are evolving from traditional SCs to extensive ecosystems, leading to complex dependencies. Effective C-SCRM requires aligning diverse perspectives within organisations. However, alignment often poses challenges within the various internal perspectives. Besides, organisations' strategic aspects are often disconnected from operational details, causing further internal alignment issues. Maya Bundt, a member of the World Economic Forum (WEF) Global Future Council on Cybersecurity, states: *"It helps when people at board level are sufficiently cyber-literate to ask pertinent questions of their security teams, but also to bring cyber into strategic business discussions. Boards also need to understand what a cyber event means for their organisation. Too many business leaders still underestimate the impact a cyberattack can have on their operations, on their reputation and on their company as a whole"* (Bueermann & Doyle, 2023, p. 16).

External alignment is equally important, highlighting the need for (digital) connectivity, real-time adjustments, and incident-handling capabilities among partners. External alignment becomes particularly significant when suppliers have access to the organisation's main infrastructure and sensitive information. Understanding different relationships and suppliers' viewpoints and expectations is essential for managing SC cyber risks effectively (Ambrose et al., 2010; Melnyk et al., 2022). The empirical results confirm that by highlighting the challenge of assessing suppliers' security posture and thus emphasising the role of relationships and trust. Power dynamics can also influence these relationships, with suppliers being aware of the consequences of not meeting security requirements including potential harm to the supplier's reputation as well as the risk of losing customers. Notably, the dominant player within an ecosystem can often set mandates, which can be the customer or the supplier, depending on the relationship. Establishing strong relationships with suppliers can be challenging due to, different perceptions of supplier and partner relationships, short contract durations and overall cost-saving. Improving these relationships requires a combination of long-term contracts, trust-building, cooperative activities beyond contracts, and supportive measures for smaller vendors. Trust and transparency are particularly important and help in effective collaboration, understanding, timely information sharing, and proactive incident response. They are fostered through certifications, dialogues, partnerships, and transparent processes. By promoting trust and transparency, SC participants can strengthen their relationships and collectively address challenges in the SC Partner Ecosystem.

The ICT components involved in organisations' CSC are shaping the attack surface that a firm and its partners face and is thus crucial to understand for effective C-SCRM. The transition from monolithic systems to integrated and automated systems has significantly expanded the attack surface and added complexity to the underlying architecture, making it difficult to grasp the dependencies fully. Here the main challenge for organisations exists in understanding the specific services a supplier provides and assessing the corresponding risks. A tier-based evaluation system or classification scheme aids in this understanding, enabling the categorisation of suppliers according to their significance and roles. However, the lack of a comprehensive view of all interdependencies was identified as an obstacle in several companies. This goes along with the findings of a PwC (2023a) survey, indicating almost a third of worldwide CISOs acknowledge a lack of architecture documentation and asset inventory especially regarding OT. Both business and technical risks need to be considered for successful C-SCRM. This includes understanding the criticality of suppliers, based on their contribution to business processes, risk levels, and the nature of their involvement. The technical assess-

ment involves understanding the network expansion through the procurement of external products/services (hardware & software SC), their connection type, and access to systems and infrastructure. Until now, organisations mainly seem to focus on the business risks.

5.3 The Demand for Standardisation and Assurance

The theoretical underpinnings of this study indicate the importance of the three main outcomes of a C-SCRM: SC Cyber Robustness, Resilience, and Assurance. Research demonstrates an expectation of balanced importance across these three outcomes, suggesting that a well-implemented C-SCRM would bolster these outcomes equally. The findings confirm this assumption. Participants acknowledge equal importance between robustness and resilience, noting that resilience may not be as equally present in widely-used standards like the ISO 27001. However, the current discussion in practice has notably shifted towards SC Cyber Assurance, which emphasises the rising demand as described by Hampton et al. (2021). This indicates that businesses may see assurance, particularly the ability to verify and prove the security of the SC to external stakeholders, as a more pressing need. This might be the result of an evolving cybersecurity landscape where trust and verification have become more valuable, due to increased regulation and intensified threat landscape around SC attacks and third-party breaches as shown in Chapter 1 of this study. While theory has highlighted the emergence of specific assurance initiatives for the CSC, e.g. by the AICPA, these seem to not have been taken up by practice yet. The interviews revealed the lack of internationally recognised standards and attestations for C-SCRM, suggesting that current practices are varied and regionally influenced. Lastly, there appears to be a contradiction in perceptions regarding the adequacy and effectiveness of current standards and assessments. The quality of certain certifications and their auditing processes was questioned, while organisations generally experience low trust in their certifications, increasing the emergence of individual practices like the use of tailored questionnaires.

Mandates in the context of C-SCRM can be instrumental in enforcing security standards and requirements across the SC ecosystem. Thus, they significantly contribute to the standardisation and assurance discussion. The theory highlights coercive pressure and signalling as effective strategies while emphasising the importance to balance mandates according to partners' reactions (Melnyk et al., 2022). Organisations commonly establish requirements through customised lists or based on established standards. Yet, there seems to be a lack of commitment and implementation on the suppliers' side and a significant overhead due to individual, non-standardised questionnaires. While there is an acknowledgement of the necessity of cybersecurity, the actual practice in implementation varies among suppliers also due to a lack of auditing and evidence gathering as mentioned under the aspect of SC Cyber Assurance.

Standards and frameworks provide an immensely valuable basis for C-SCRM, as theoretically, they offer a common starting point and understanding of cybersecurity measures (Davis, 2015). While the use of standards is seen as beneficial to introduce a common baseline, the empirical evidence, however, indicates that while there is widespread use of generic standards such as ISO 27000 and NIST CSF, their effectiveness in assuring comprehensive SC cybersecurity is limited. The dominance of these standards showing a scoping issue towards SC cybersecurity and the lack of specific C-SCRM standards were highlighted. The majority of the participants propose the development of standardised requirements at a European or sector level to avoid competing sets of requirements and enhance effectiveness.

Part of all the standards mentioned before is to ground them on common security objectives. The theoretical

literature on C-SCRM emphasises the importance of defining security objectives that extend beyond the CIA-Triad to account for the unique cyber risks present in SCs (Windelberg, 2016; Boyes, 2015; Sawik, 2022a). Specifically, scholars suggest adopting the Parkerian Hexad. The empirical findings, however, reveal a disparency between the theoretical and practical approaches. Although there is general agreement among our participants about the necessity to extend the CIA-Triad with business continuity, disaster recovery, and crisis management objectives, the highly theoretical viewpoint to precisely differentiate between the objectives is not taken up by the interviewees. Participants primarily emphasise the broad applicability of these objectives, ensuring they consistently align with the three foundational objectives. Furthermore, the lack of clarity in recent iterations of ISO 27001 concerning the extension towards resilience is also highlighted as a barrier in practice.

Notably, upcoming EU regulations, such as NIS2 and CRA, are seen as potential game-changers in imposing stricter requirements on SC cybersecurity. However, the efficacy of these regulations is a matter of debate among the participants, as their impact can range from minimal compliance to inducing comprehensive improvements in SC security. Especially their transposition and enforcement on a national level remain open. This goes along with the survey results of the WEF, where 70% of business and cyber leaders opt for stricter enforcement of regulatory requirements to enhance the resilience of SCs (Bueermann & Doyle, 2023).

5.4 Expand Collaboration and Consider Shared Investments

The role of collaboration in C-SCRM has been substantiated both theoretically and practically. The theoretical underpinnings indicate that collaboration is integral to resilience and encompasses activities such as inter alia, information sharing, joint-decision making or resource sharing (Colicchia et al., 2019; Ghadge et al., 2020; Boyens et al., 2022). Collaboration may occur both vertically, involving suppliers or customers, and horizontally, with competitors or other partners (Singh et al., 2018). The empirical findings of this study reinforce the significance of collaboration in the context of C-SCRM. Collaborative efforts allow for shared goals against common adversaries, improved defence strategies, the pooling of expertise, alignment of perspectives, and compliance among a larger group of organisations. Trust is underscored as a critical success factor of collaboration, necessitating the establishment and maintenance of robust relationships. Modes of collaboration that have been successfully implemented include inter-company groups, sector-wide initiatives, and partnerships for cybersecurity innovation. Concerns and challenges emerge within sensitive environments, the absence of governance structures to facilitate collaboration and potential legal consequences of information or knowledge sharing. Notably, coordinated cybersecurity investments together with suppliers were not seen as a possible solution to the challenge of funding collaboration initiatives.

Cybersecurity investments play a critical role in supporting C-SCRM efforts. Theoretically, coordinated investments across the SC are essential for effective C-SCRM (Sawik, 2022a, 2022b; Simon & Omar, 2020). However, empirical findings show that there are yet no sound coordination mechanisms defined in practice. Even though initiatives exist, such as shared response services or the development of a shared Security Operations Center (SOC) with strategic suppliers, these are not widespread and rather seen as collaboration initiatives. Long-term contractual relationships are identified as one of the major vehicles for fostering such partnerships within the SC. Cybersecurity investments and collaboration are found to be closely related in practice, however not showing clearly defined mechanisms in their approaches.

5.5 Challenges of True Visibility & Flexibility

Following the definition by Jüttner and Maklan (2011), SC visibility is conceptualised as the extent to which key actors within the SC have timely access to or share information about SC operations, other actors, and management. This information is considered essential for effective C-SCRM, particularly given the risks stemming from actors and ICT components beyond tier 1 of the SC (Garvey et al., 2021). Empirical findings corroborate this theoretical understanding of the importance of SC visibility. Our interview participants agreed on the importance of obtaining a comprehensive understanding of the entire SC ecosystem, including multiple layers of suppliers and sub-contractors. However, they also highlighted the considerable challenge in achieving this level of visibility and admitted the missing visibility as described in theory. Current efforts are predominantly driven by legal requirements, such as GDPR, and are mostly targeted towards a select group of critical suppliers. Additionally, the lack of formal contracts and relationships with sub-suppliers make it difficult for firms to acquire necessary information due to the absence of a contractual obligation and amplifies the resource constraints. Organisations are mainly focusing on incorporating contractual clauses obligating suppliers to share information about their sub-contractors, extending certification requirements to sub-suppliers, and major market players acquiring their key suppliers to have them within their internal ecosystem. Notably, the Program Manager highlighted the importance of developing shared incident-handling and information-sharing capabilities, rather than striving for exhaustive visibility that may be impractical given the complexity and extent of modern SCs.

The theoretical implications of Organisational Agility, consisting of the intertwined concepts of SC Agility and SC Flexibility, propose that businesses should be equipped with the capability to alter their SC structure swiftly and efficiently, under C-SCRM. Contrarily, the empirical evidence from the interviews reveals that implementation of the two concepts appears to be less straightforward. Participants agreed on the broad idea of flexibility/ agility and its importance but encountered operational-level challenges when it came to implementation. Specifically, many found that switching suppliers during disruptions was not only operationally difficult but also costly due to strong dependencies, particularly in long-term and highly integrated relations. The idea of a multi-vendor approach, theoretically sound, seemed to lose its feasibility in reality due to limited availabilities during widespread disruptions and high effort to facilitate the switch. Participants also highlighted the perceived trend of supplier consolidation due to efficiency reasons. However, promising findings reveal that agility and flexibility are not completely unachievable. Some organisations have initiated strategies to boost their organisational agility, such as developing exit and replacement strategies aligned with procurement policies, and continuous monitoring of supplier alternatives. Large organisations may increase control over SC cyber risks by integrating critical suppliers through firm acquisitions.

From a theoretical lens, situational awareness involves understanding potential cyber threats, vulnerabilities, and risks within an organisation and its extended SC ecosystem (Colicchia et al., 2019; Guerra & Estay, 2019). This knowledge enables organisations to act strategically in the face of cybersecurity threats. The importance is acknowledged by the participants but shows differences in practical implementation. Empirical evidence from the interviews underlines the challenges organisations face in maintaining this awareness and highlight situational awareness as a crucial area for improvement. The participants indicated limited formal processes for staying aware of suppliers' security posture changes and recent vulnerabilities. Methods used often include external resources such as annual security analyses, collaborations with government agencies, using external platforms like BitSight, subscribing to threat intelligence feeds, and participating in Information

Sharing and Analysis Centers (ISACs). However, structured monitoring, especially regarding Information Technology (IT) and Operational Technology (OT) systems, is lacking but is seen as necessary for successful C-SCRM. The consistency of the assessed posture over time is also seen as crucial yet challenging.

Finally, cybersecurity readiness in theory encompasses a variety of technological, environmental, and organisational aspects (Hasan et al., 2021). The empirical findings, however, indicate a struggle among participants to conceptualise cybersecurity readiness holistically. Several participants stressed the need to integrate C-SCRM proactively into overall security programs and address it as a key part of information security initiatives. They also underscored the necessity to adopt a risk-driven approach over a compliance-oriented approach, necessitating board-level involvement and comprehensive governance structures. Moreover, it was highlighted that not all risks can be mitigated solely by securing the SC. Organisations must define processes for handling incidents and vulnerabilities, emphasising the role of operational readiness as highlighted under the aspect of SC Visibility. Technical readiness was also identified as key, including proper documentation and management of existing architecture. Thus, the concepts were renamed as *"Organisational C-SCRM Prerequisites"* under the structural elements as described in Section 4.3.

6 | Conclusion

This thesis gives a comprehensive overview of the complexities of modern (cyber) SCs and the rising risks with associated cyber threats. In light of the regulatory pressure imposed by existing and forthcoming EU regulations, it has become evident that organisations must take action. Research shows that current initiatives are not sufficient to counter advanced threats that exploit the weakest link in a SC ecosystem. The notion of C-SCRM provides a possible approach, but its implementation in practice remains relatively unexplored. Therefore, this thesis aims to answer four main research questions. First, it was tried to investigate *"Which primary research topics and concepts about C-SCRM have been investigated in prior research?"* (RQ1). Following that, the concepts were used to answer *"What are structural elements and drivers for successful implementation and operation of an organisational C-SCRM?"* (RQ2). RQ3 aimed to explore *"What is the operational state of C-SCRM in organisations within the Netherlands?"*. Finally, RQ4 investigated *"How are the structural elements and drivers for C-SCRM perceived in practice?"*. By that, this thesis presents, to the author's best knowledge and belief, one of the most detailed publications around C-SCRM and displays the most up-to-date picture of organisational initiatives in the Netherlands. This work provides a conceptualisation of the overarching issue and investigates how related concepts can be leveraged in detail. Thus, this work is both insightful for practitioners and provides a cornerstone for future studies.

Chapter 2 of this study addressed the first two research questions (RQ1 & RQ2). The most researched themes in C-SCRM literature were the nature of different SC cyber risks and threats, corresponding mitigation strategies and challenges in C-SCRM. Furthermore, a variety of publications tried to define relevant terminologies in the field, which are still lacking. This study tried to combine existing perspectives to contribute to a shared paradigm for the notion of the CSC and C-SCRM. The results of the review were used to establish a conceptual framework addressing RQ2. The framework presents a holistic perspective on structural elements and drivers that influence an organisational C-SCRM. The framework outlines structural elements to understand and analyse a CSC prior to developing a C-SCRM, drivers that impact the performance, and desired main outcomes from a successful C-SCRM. Semi-structured interviews were used to investigate the established conceptual framework. RQ3 and RQ4 are answered in the results (Chapter 4) and subsequent discussion (Chapter 5) of the interviews. The findings indicate a rising awareness about the problem on a board level, also due to the severity of recent attacks, raising the question: *"Could this happen to us" (Cybersecurity Architect)?* Simultaneously, C-SCRM is deemed as *"one of the hardest topics in security" (CISO)*. However, organisations currently lack the needed governance structures and resources to implement a holistic C-SCRM. ENISA, who answered selected interview questions in writing, underscores the missing standards and best practices as the main reason for the difficulties and slow progress. This lack is amplified by a poor understanding of ICT dependencies and missing cross-functional knowledge and that's why *"only a few organisations actually started improving (Consultant-1)"*. Current comprehensive initiatives in the Netherlands are restricted to large mature organisations or firms operating in very sensitive environments. They can be seen as pioneers, working without best practices and still requiring a lot of resources. Most of the initiatives are limited to the first tier of suppliers and solely address the business risk in case

of a disruption. Considering RQ4, the research indicates that organising concepts into structural elements, drivers, and main outcomes enhances the contextual understanding of the conceptual framework. However, the proposed categorisation into mediating and moderating elements was not validated and was therefore dismissed. The findings underscored the importance of structural elements as a precondition for developing a comprehensive C-SCRM. Several participants see risk assessments and understanding relevant dependencies as the biggest challenge. While standards, frameworks, mandates, and collaboration are recognised and utilised by practitioners, coordinated investments, situational awareness, and a clear definition of C-SCRM objectives are less well-established and understood in practice. SC agility/flexibility and SC visibility are deemed vital for C-SCRM but pose significant practical implementation challenges.

Much like the statement by David Koh, presented in Chapter 1 of this thesis, the results highlight the importance and urgency of safeguarding the CSC, underscoring it as a matter of concern at the board level. Nevertheless, an examination of the implementation reveals that companies cannot presently keep up with the rapid pace set by threat actors. The structural elements and drivers outlined, enable organisations to effectively compete in this race.

In the remainder of this chapter, we further detail theoretical and practical implications in Sections 6.1 and 6.2. In Section 6.3, we present the limitations of this thesis and directions for future work.

6.1 Theoretical Implications

Several implications for research can be derived from the presented findings. The literature on C-SCRM, particularly from industry publications, has been noticeably expanding, a trend observed even during the writing of this thesis. However, it appears that in practice, C-SCRM is often not recognised as a distinct field but is viewed through the lens of SC risk management or vendor risk management. This highlights the need for clear boundaries and overlaps to better distinguish C-SCRM from related areas, also in research. In essence, this study amplifies earlier studies concerning C-SCRM and the challenges associated with it. While this study confirmed the relevance of several concepts introduced by other publications, it also noted that some concepts, such as cybersecurity readiness, are not yet well-translated into practice. Moreover, previous studies tend to focus on specific mitigation strategies. The findings of this study highlight that a major challenge lies in analysing and understanding the complexities of the SC ecosystems. Moreover, current methodologies and frameworks in the literature do not appear to be widely recognised or implemented in practical settings as of yet. Research needs to evolve towards the implementation and evaluation of C-SCRM.

6.2 Practical Implications

Additionally, the findings include several implications for practice. The results reveal a rising willingness among organisations to engage in robust C-SCRM practices. However, it appears that they miss the required tools and knowledge to drive those initiatives. On the other hand, the results suggest that the primary focus of businesses should be to strengthen their partnerships, laying special emphasis on fostering trust and transparency. This approach, particularly for SMEs, could serve as a central cornerstone for the incremental implementation of C-SCRM. There is a potential opportunity to leverage CYRA in the Netherlands, promoting a market-driven standardisation that could support organisations in this journey. Furthermore, new EU regulations will likely exert increased pressure on organisations to augment their efforts in C-SCRM.

This outlook will require the establishment of effective governance structures and the development of best practices to guide these enhanced security efforts. Thus, there is a growing demand for advisory services to help businesses comprehend the emerging requirements and complexities in SCs and guide implementation. The results further highlight the crucial role that new market participants could play in bolstering organisational initiatives. This includes the provision of e.g. assurance services and continuous monitoring.

6.3 Limitations & Future Research

This thesis is subject to different limitations, partly addressed in the description of the scope in Section 1.4. This study primarily aims to provide a comprehensive perspective on the topic and C-SCRM initiatives from an organisational perspective. However, it does not delve into certain alternative solutions, such as technological tools like the software bill of materials, which could potentially contribute significantly to the mitigation of a number of software-related SC attacks. The study's scope is limited by the number of interviews conducted and the specificity of interview questions. This limitation further restricts the precision of the conclusions, preventing the identification of a universally applicable best practice approach for organisations. The most significant constraint of this study lies in the fact that its scope does not permit an exhaustive validation of the individual concepts. Further quantitative studies examining the specific impact of these concepts would be beneficial for the strategic implementation. Consequently, this study does not evaluate the significance of these concepts in relation to C-SCRM. Moreover, this study aims to establish a holistic understanding.

The presented findings and limitations revealed several future research directions. These could include investigations into solutions that simplify the entanglements within SCs. In particular, there is a need to differentiate and categorise various outsourcing scenarios, along with their respective cybersecurity implications. Used terminology remains inconsistent and has to be aligned. Further exploration is also needed to pinpoint exact overlaps between existing efforts in SC risk management, vendor risk management, and other disciplines that could be utilised for C-SCRM. It is crucial not only to define what C-SCRM encapsulates but also to clarify what it does not, in order to delineate its boundaries more effectively. Studies evaluating implementation methodologies and roadmaps for C-SCRM within organisations could be valuable, as they might help identify best practices at the organisational level. Furthermore, the research around metrics to evaluate good C-SCRM practices can provide actionable insights to improve risk mitigation.

7 | Recommendations

The growing threat landscape through SC attacks and upcoming regulations forces organisations to act on their SC cybersecurity. This study revealed shortcomings in the progress of developing adequate solutions to keep up with the evolving risk landscape. It has become evident, that collaborative action is needed to enhance maturity around SC cybersecurity in practice, ultimately aiming to enhance robustness, resilience and assurance of the CSC. A possible approach is a symbiosis of developing an organisational C-SCRM, utilising managed security services and driving standardisation within the field of SC cybersecurity. In this chapter, we provide recommendations to the different stakeholders in the Netherlands to facilitate this development. These are: organisations willing to implement C-SCRM, external consultancies and service providers, and policy makers. The accompanying thesis identified these three stakeholders as facilitators to drive the needed developments in the context of SC cybersecurity. The provided recommendations present a synthesis of the findings from this study as well as insights of current industry publications.

Organisations implementing C-SCRM

Organisations planning to implement a C-SCRM can take several proactive steps immediately. First, it is recommended to establish a **centralised** C-SCRM rooted in a dedicated strategy and underpinned by clearly defined organisational structures. Therefore, it is crucial to enhance the **collaboration** on the board level to ensure commitment and strategic guidance. However, bridging the communication gap between cyber and business leaders presents the foundation to make the return on investment of C-SCRM understandable. It is important to internalise that C-SCRM is not a compliance exercise and only effective through a risk-driven approach. The cornerstone of C-SCRM is a sound **SC risk management** procedure including professionals from across the organisation focusing on ICT and OT risks. A **standard-oriented approach** should be preferred that fits existing cybersecurity efforts, accompanied by an **open communication** regarding potential risks. The definition of clear **responsibilities** internally, as well as with suppliers is of major importance. In this context, organisations should include audit rights, notification obligations, general information sharing, and the handling of sub-contractors in the discussion with suppliers. Strengthening of existing supplier **relationships** by focusing on **transparency and trust** will amplify collaboration with suppliers and ensure a rapid incident response. Collaboration, especially including information and knowledge sharing is indispensable for successful C-SCRM. While continuing to raise organisational-wide awareness and enhancing internal knowledge, organisations should consider building external **monitoring capabilities** with a focus on resilience, optimally as shared investments with close suppliers. Finally, organisations should carefully define **security requirements** for their acquired products and services and ensure to retain transparent and complete documentation of their **enterprise architecture**.

In light of the enforcement of NIS2 from October 2024 on, organisations are recommended to act immediately. To reach NIS2 compliance regarding the requirements for SC security, organisations mainly have to address four aspects in their SCs (adapted and tailored from Papaphilippou et al. (2023)):

- SC risk management
- Management of the SC partner ecosystem and corresponding relationships including insights in in the dependence of 1st, 2nd, n-tier suppliers.
- Vulnerability and incident handling in products and services
- Ensure the quality of products and cybersecurity measures of service providers

The activities discussed can be mapped onto a Plan-Do-Check-Act (PDCA) cycle, as illustrated in Figure VIII, a framework often employed in information security management systems such as ISO 27001. This iterative cycle is designed to promote continuous improvement. The figure is further extended to indicate how the concepts examined in this study can aid organisations in sustaining the practices included in the cycle. Note that the selection is not meant to be exclusive.

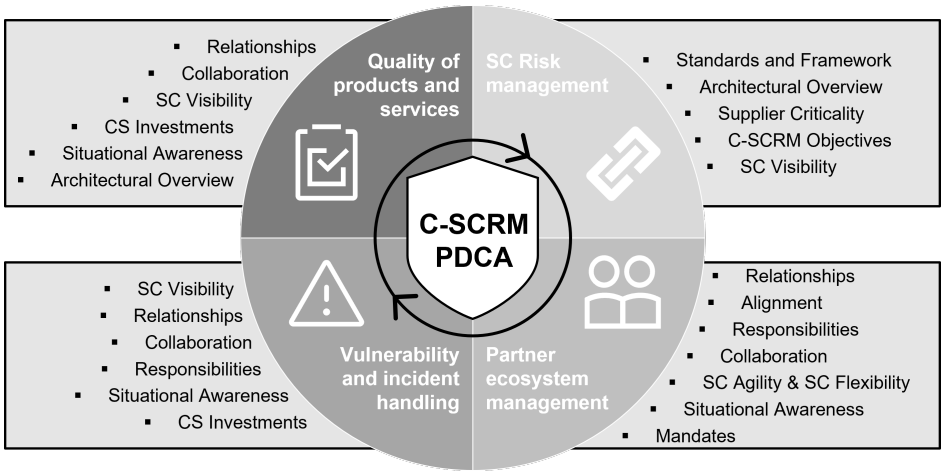

FIGURE VIII. C-SCRM PDCA Cycle. Own illustration, adapted from Papaphilippou et al. (2023).

Additionally, organisations might already prepare the implementation of supplementary requirements by the upcoming CRA. By that it can be recommended to perform a broad estimation if the scope will apply to the organisation. Respective risk management procedures to evaluate the quality of suppliers products and services in the scope of NIS2 might be subsequently designed to also apply for the organisations own products and services. As the risk management procedures are required throughout the whole system development lifecycle, the requirements of the two regulations complement each other. Although the reporting obligations for the CRA are not yet precisely defined, it can be recommended to emphasise the development of comprehensive reporting procedures not only for incidents but also exploited vulnerabilities.

External consultancies and service providers

This study found an increasing demand for external consultancies and cybersecurity service providers to aid organisations on the way to developing and maintaining a C-SCRM. Consultancies are recommended to develop **holistic service offerings** to guide organisations. Especially the interpretation and transposition of regulatory requirements into practice are in high demand. **Advisory on board level** can aid the alignment of the different perspectives, resulting in effective strategy development. Specific **sector knowledge** can help to advise clients on best practices and leverage existing possibilities in their ecosystems. Furthermore, there is a demand for cybersecurity service providers to develop security solutions that minimise effort and are easily accessible also for non-cybersecurity professionals. Products and services are needed that help

organisations to **simplify the complexities** in the SC and **provide visibility** with the least amount of effort. Furthermore, recent technology developments can be used to enhance **security monitoring** of suppliers and develop **predictive risk indicators**.

Policymakers

Policymakers on the EU and national level are recommended to **drive standardisation** in regard to SC cybersecurity. Standards and regulations are needed and welcomed, however, policymakers should ensure **harmonisation** with existing regulations and seek **industry collaboration** on a sector level. Regulations should focus on the implementation and operation of effective controls and their enforcement rather than compliance, as emphasised in the quote by Hoda Al Khzaimi below. By pointing to **established industry standards** policymakers can support organisations to operationalise regulatory requirements and highlight that in its core, legislation should always be about the effectiveness of cybersecurity. Last but not least it is recommended to further **strengthen cybersecurity education** to overcome the staff shortage. Part of this is the misconception of cybersecurity as a purely technical domain. Especially SC cybersecurity needs generalist roles with a broader skillset, being able to mediate business and tech leaders.

> *"The way we build regulations for cybersecurity is centralised. The regulations this system creates are valuable, but the process takes time. It can take two years for a regulation to be developed. Standardisation can take 18 months. A cyberattack takes seconds. The speed at which emerging technologies are implemented often outpaces our ability to build security measures around them. We need to go beyond simple compliance with regulations if organisations are to be cyber resilient."*
> Hoda Al Khzaimi, Director, Center for Cybersecurity, New York University (NYU) (2023, p. 13).

References

Alshurideh, M. T., Alquqa, E. K., Alzoubi, H. M., Kurdi, B. A., & Alhamad, A. (2023, 12). The impact of cyber resilience and robustness on supply chain performance: Evidence from the uae chemical industry. *Uncertain Supply Chain Management*, *11*, 187-194. doi: 10.5267/j.uscm.2022.10.008

Ambrose, E., Marshall, D., & Lynch, D. (2010). Buyer supplier perspectives on supply chain relationships. *International Journal of Operations and Production Management*, *30*, 1269-1290. doi: 10.1108/01443571011094262

Baiardi, F., Tonelli, F., Bertolini, A., & Montecucco, M. (2016). Metrics for cyber robustness. *NATO Science and Technology Organization*, 1-18.

Bandara, E., Tosh, D., Shetty, S., & Krishnappa, B. (2021). Cyscpro - cyber supply chain provenance framework for risk management of energy delivery systems. In *Proceedings - 2021 ieee international conference on blockchain, blockchain 2021* (p. 65-72). doi: 10.1109/Blockchain53845.2021.00020

Bartol, N. (2014). Cyber supply chain security practices dna - filling in the puzzle using a diverse set of disciplines. *Technovation*, *34*, 354-361. doi: 10.1016/j.technovation.2014.01.005

Bode, C., & Wagner, S. M. (2015, 5). Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. *Journal of Operations Management*, *36*, 215-228. doi: 10.1016/j.jom.2014.12.004

Boyens, J., Paulsen, C., Bartol, N., Shankles, S. A., & Moorthy, R. (2012, 10). *Notional supply chain risk management practices for federal information systems.* Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf doi: 10.6028/NIST.IR.7622

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2020, 2). *Case studies in cyber supply chain risk management: Summary of findings and recommendations.* Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-1.pdf doi: 10.6028/NIST.CSWP.02042020-1

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2021, 2). *Nistir 8276 - key practices in cyber supply chain risk management: Observations from industry.* Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf doi: 10.6028/NIST.IR.8276

Boyens, J., Smith, A., Bartol, N., Holbrook, K., & Fallon, M. (2022). *Nist sp 800-161r1 - cybersecurity supply chain risk management for systems and organizations.* Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf doi: 10.6028/NIST.SP.800-161r1

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, *5*, 28-34. doi: http://doi.org/10.22215/timreview/888

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems. *Technovation*, *34*, 342-353. doi: 10.1016/j.technovation.2014.02.001

Boyson, S., Corsi, T., & Paraskevas, J.-P. (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation*, *118*. doi: 10.1016/j.technovation.2021.102380

Bueermann, G., & Doyle, S. (2023). *Global cybersecurity outlook 2023.* Geneva, CH: World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Carter, C. R., Rogers, D. S., & Choi, T. Y. (2015, 4). Toward the theory of the supply chain. *Journal of Supply Chain Management*, *51*, 89-97. doi: 10.1111/jscm.12073

Cha, S. (2022). The art of cyber security in the age of the digital supply chain. In *The digital supply chain* (p. 215-233). Elsevir. doi: 10.1016/B978-0-323-91614-1.00013-7

Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021, 2). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*. doi: 10.1016/j.tre.2020.102217

Chiara, P. G. (2022). The cyber resilience act: the eu commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*, *3*, 255-272. doi: 10.1365/s43439-022-00067-6

Colicchia, C., Creazza, A., & Menachof, D. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management*, *24*, 215-240. doi: 10.1108/SCM-09-2017-0289

Commitee on Commerce, Science, and Transportation. (2014). *A "kill chain" analysis of the 2013 target data breach.* Retrieved from https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883

Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*.

Cox, K., Jolly, S., & Staaij, S. V. D. (2018). *Understanding the drivers of organisational capacity.* Santa Monica, CA: RAND Corporation.

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, *27*, 30-53. doi: 10.1108/SCM-02-2020-0073

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (Fourth Edition ed.). Boston, MA: Pearson Education, Inc.

Davidson, D., & Shankles, S. (2013). We cannot blindly reap the benefits of a globalized ict supply chain! *CrossTalk*, *26*, 4-7.

Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, *5*, 19-27.

Deane, J., Baker, W., & Rees, L. (2022). Cybersecurity in supply chains: Quantifying risk. *Journal of Computer Information Systems*. doi: 10.1080/08874417.2022.2081882

Eckhardt, P., & Kotovskaia, A. (2023). The eu's cybersecurity framework: the interplay between the cyber resilience act and the nis 2 directive. *International Cybersecurity Law Review*, *4*, 147-164. doi: 10.1365/s43439-023-00084-z

ENISA. (2021). *Enisa threat landscape for supply chain attacks.* Athens: European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Fayezi, S., Zutshi, A., & O'Loughlin, A. (2017). Understanding and development of supply chain agility and

flexibility: A structured literature review. *International Journal of Management Reviews*, *19*, 379-407. doi: 10.1111/ijmr.12096

Fernando, Y., Tseng, M. L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Jabbour, C. J. C., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in malaysia. *Journal of Industrial and Production Engineering*, *40*, 102-116. doi: 10.1080/21681015.2022.2116495

Filho, N., Rego, N., & Claro, J. (2021). Supply chain flows and stocks as entry points for cyber-risks. In *Procedia computer science* (Vol. 181, p. 261-268). doi: 10.1016/j.procs.2021.01.145

Gani, A., & Fernando, Y. (2018). Concept and practices of cyber supply chain in manufacturing context. In M. Khosrow-Pour (Ed.), *Encyclopedia of information science and technology* (Fourth Edition ed., Vol. VII, p. 5306-5316). IGI Global.

Gani, A., Fernando, Y., Lan, S., Lim, M., & Tseng, M.-L. (2023). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management and Data Systems*, *123*, 843-861. doi: 10.1108/IMDS-05-2022-0313

GAO. (2012). *It supply chain national security-related agencies need to better address risks report to congressional requesters.* United States Government Accountability Office.

Garvey, M. D., Samuel, J., & Kretinin, A. (2021). An ontology of supply chain cybersecurity. In S. Carnovale & S. Yeniyurt (Eds.), *Cyber security and supply chain management risks, challenges, and solutions* (Vol. 1, p. 71-132). World Scientific Publishing.

Ghadge, A., Weiß, M., Caldwell, N., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, *25*, 223-240. doi: 10.1108/SCM-10-2018-0357

Greenberg, A. (2023). *The huge 3cx breach was actually 2 linked supply chain attacks.* Wired. Retrieved from https://www.wired.com/story/3cx-supply-chain-attack-times-two/ (Acessed on 20.07.2023)

Greenwald, G. (2014). *Glenn greenwald: how the nsa tampers with us-made internet routers.* The Guardian. Retrieved from https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (Acessed on 20.07.2023)

Guba, E. G. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *ECTJ*, *29*, 75-91.

Guerra, P., & Estay, D. S. (2019). An impact-wave analogy for managing cyber risks in supply chains. *IEEE International Conference on Industrial Engineering and Engineering Management*, *2019-Decem*, 61-65. doi: 10.1109/IEEM.2018.8607563

Hampton, C., Sutton, S., Arnold, V., & Khazanchi, D. (2021). Cyber supply chain risk management: Toward an understanding of the antecedents to demand for assurance. *Journal of Information Systems*, *35*, 37-60. doi: 10.2308/ISYS-19-050

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. doi: 10.1016/j.jisa.2020.102726

ISC. (2022). *Cybersecurity workforce study 2022: A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution.* International Information System Security Certification Consortium. Retrieved from https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, *8*, 49-62. doi: 10.1177/160940690900800406

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). *Nist sp 800-150:*

Guide to cyber threat information sharing. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf doi: 10.6028/NIST.SP.800-150

Jones, C. (2021). *Warnings (& lessons) of the 2013 target data breach.* Retrieved from https://redriver.com/security/target-data-breach (Acessed on 19.07.2023)

Juniper Research Ltd. (2023). *Vulnerable software supply chains are a multi-billion dollar problem.* Hampshire, UK: Juniper Research Ltd. Retrieved from https://www.juniperresearch.com/whitepapers/vulnerable-software-supply-chains-problem

Jüttner, U., & Maklan, S. (2011). Supply chain resilience in the global financial crisis: An empirical study. *Supply Chain Management*, *16*, 246-259. doi: 10.1108/13598541111139062

Kim, K. C., & Im, I. (2014). Research letter: Issues of cyber supply chain security in korea. *Technovation*, *34*, 387-388. doi: 10.1016/j.technovation.2014.01.003

Kovacs, E. (2021). *Solarwinds agrees to pay $26 million to settle shareholder lawsuit over data breach.* SecurityWeek. Retrieved from https://www.securityweek.com/solarwinds-agrees-pay-26-million-settle-shareholder-lawsuit-over-data-breach/ (Acessed on 19.07.2023)

Küffner, C., Kopyto, M., Wohlleber, A. J., & Hartmann, E. (2022, 11). The interplay between relationships, technologies and organizational structures in enhancing supply chain resilience: empirical evidence from a delphi study. *International Journal of Physical Distribution and Logistics Management*, *52*, 673-699. doi: 10.1108/IJPDLM-07-2021-0303

Lu, T., Yao, P., Guo, X., Zhang, X., Zhao, L., & Yang, H. (2015). A systematic study for ict supply chain security. *Journal of Logistics, Informatics and Service Science*, *Vol. 2*, 28-41.

Ludvigsen, K. R., Nagaraja, S., & Daly, A. (2022, 11). Preventing or mitigating adversarial supply chain attacks. In *Proceedings of the 2022 acm workshop on software supply chain offensive research and ecosystem defenses* (p. 25-34). New York, NY, USA: ACM. doi: 10.1145/3560835.3564552

Makri, C., & Neely, A. (2021). Grounded theory: A guide for exploratory studies in management research. *International Journal of Qualitative Methods*, *20*. doi: 10.1177/16094069211013654

Martin, R. A. (2020). The supply chain security system of trust: A framework for the concerns blocking trust in supplies, suppliers, and services. *Cutter Business Technology Journal*, *33*, 28-36.

Martínez, J., & Durán, J. (2021). Software supply chain attacks, a threat to global cybersecurity: Solarwinds' case study. *International Journal of Safety and Security Engineering*, *11*, 537-545. doi: 10.18280/IJSSE.110505

Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., ... Kalogiannis, G. (2021). Cybersecurity in ict supply chains: Key challenges and a relevant architecture. *Sensors*, *21*. doi: 10.3390/s21186057

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022, 1). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*, 162-183. doi: 10.1080/00207543.2021.1984606

Miller, J. F. (2013). *Supply chain attack framework and attack patterns.* McLean, VA: MITRE Corporation.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the prisma statement. *BMJ*, *339*, b2535-b2535. doi: 10.1136/bmj.b2535

NCTV. (2022a). *Action plan - netherlands cybersecurity strategy 2022-2028: Ambitions and actions for a digitally secure society.* The Hague, NL: National Coordinator for Counterterrorism and Security. Retrieved from https://english.nctv.nl/topics/netherlands-cybersecurity-strategy

-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy--action-plan

NCTV. (2022b). *Netherlands cybersecurity strategy 2022-2028: Ambitions and actions for a digitally secure society.* The Hague, NL: National Coordinator for Counterterrorism and Security. Retrieved from https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028

NCTV. (2023). *Cyber security assessment netherlands 2023.* The Hague, NL: National Coordinator for Security and Counterterrorism. Retrieved from https://english.nctv.nl/documents/publications/2023/07/03/cyber-security-assessment-netherlands-2023

NDIA. (2008). *Engineering for system assurance.* Arlington, Virginia: National Defense Industrial Association System Assurance Committee. Retrieved from https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.ashx

Nygård, A., & Katsikas, S. (2022). Sok: Combating threats in the digital supply chain. In *Acm international conference proceeding series.* doi: 10.1145/3538969.3544421

Pandey, S., Singh, R., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*, 103-128. doi: 10.1108/JGOSS-05-2019-0042

Papaphilippou, M., Moulinos, K., & Theocharidou, M. (2023). *Good practices for supply chain cybersecurity.* European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity doi: 10.2824/805268

Pipikaite, A. (2022). *Global cybersecurity outlook 2022.* Geneva, CH: World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

PwC. (2023a). *A c-suite united on cyber-ready futures: Findings from the 2023 global digital trust insights.* United States: PricewaterhouseCoopers. Retrieved from https://www.pwc.com/us/en/forms/2023-global-digital-trust-insights-download.html

PwC. (2023b). *Cyber threats 2022: A year in retrospect.* PricewaterhouseCoopers. Retrieved from https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

Pérez-Morón, J. (2022, 3). Eleven years of cyberattacks on chinese supply chains in an era of cyber warfare, a review and future research agenda. *Journal of Asia Business Studies*, *16*, 371-395. (just for introduction) doi: 10.1108/JABS-11-2020-0444

Robertson, J., & Riley, M. (2018). *The big hack: How china used a tiny chip to infiltrate u.s. companies.* Bloomberg. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies (Acessed on 20.07.2023)

Satter, R. (2021). *Solarwinds says dealing with hack fallout cost at least $18 million.* Reuters. Retrieved from https://www.reuters.com/technology/solarwinds-says-dealing-with-hack-fallout-cost-least-18-million-2021-04-13/ (Acessed on 19.07.2023)

Saunders, M., Lewis, P., & Thornhill, A. (2019a). Collecting primary data using research interviews and research diaries. In (Eighth Edition ed., p. 434-464). New York: Pearson Education, Limited.

Saunders, M., Lewis, P., & Thornhill, A. (2019b). Formulating the research design. In (Eighth Edition ed., p. 172-231). New York: Pearson Education, Limited.

Saunders, M., Lewis, P., & Thornhill, A. (2019c). Negotiating access and research ethics. In (Eighth Edition ed., p. 232-291). New York: Pearson Education, Limited.

Sawik, T. (2022a). Balancing cybersecurity in a supply chain under direct and indirect cyber risks. *International Journal of Production Research*, *60*, 766-782. doi: 10.1080/00207543.2021.1914356

Sawik, T. (2022b). A linear model for optimal cybersecurity investment in industry 4.0 supply chains. *International Journal of Production Research*, *60*, 1368-1385. doi: 10.1080/00207543.2020.1856442

Saxe, J. G. (1872). *The blind man and the elephant.*

Schauer, S., Polemi, N., & Mouratidis, H. (2019). Mitigate: a dynamic supply chain cyber risk assessment methodology. *Journal of Transportation Security*, *12*, 1-35. doi: doi:10.1007/s12198-018-0195-z

Scholten, K., & Schilder, S. (2015). The role of collaboration in supply chain resilience. *Supply Chain Management*, *20*, 471-484. doi: 10.1108/SCM-11-2014-0386

Shah, S. (2021). *The financial impact of solarwinds breach.* BitSight. Retrieved from https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided (Acessed on 19.07.2023)

Shankles, S., Moss, M., Pickel, J., & Bartol, N. (2013). How international standard efforts help address challenges in today's global ict marketplace. *CrossTalk*, *26*, 10-15.

Shoemaker, D., III, J. R., & Wilson, C. (2012). A governance framework for ict supply chain risk management. *EDPACS*, *46*, 1-8. doi: 10.1080/07366981.2012.748557

Shoemaker, D., & Mead, N. (2013). Building a body of knowledge for ict supply chain risk management. *CrossTalk*, *26*, 24-28.

Shoemaker, D., & Wilson, C. (2013). The weakest link-the ict supply chain and information warfare. In *8th international conference on information warfare and security, iciw 2013* (p. 208-214).

Siciliano, G., & Gaudenzi, B. (2018). The role of supply chain resilience on it and cyber disruptions. *Lecture Notes in Information Systems and Organisation*, *24*, 57-69. doi: 10.1007/978-3-319-62636-9_4

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*, 161-171. doi: 10.1016/j.ejor.2019.09.017

Simpson, S., Baldini, D., Bitz, N. G., Dillard, D., Fagan, C., & Reddy, D. (2010). *Software integrity controls an assurance-based approach to minimizing risks in the software supply chain.* SAFECode. Retrieved from https://safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf

Simpson, S., Reddy, D., Minnis, B., Networks, J., Fagan, C., Mcguire, M. C. C., ... Ii, S. (2009). *The software supply chain integrity framework defining risks and responsibilities for securing software in the global supply chain.* SAFECode. Retrieved from http://safecode.org/publication/SAFECode_Supply_Chain0709.pdf

Singh, H., Garg, R. K., & Sachdeva, A. (2018). Supply chain collaboration: A state-of-the-art literature review. *Uncertain Supply Chain Management*, *6*, 149-180. doi: 10.5267/j.uscm.2017.8.002

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics (Switzerland)*, *9*, 1-31. doi: 10.3390/electronics9111864

Splunk Inc. (2023). *The state of security 2023 - global research: How leading organizations engage the entire business to build resilience.* San Francisco, CA: Splunk Inc. Retrieved from https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2023.pdf

Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers and Security*, *108*. doi: 10.1016/j.cose.2021.102324

van den Brink, P., Duijnhoven, H., Melman, I., Poppink, B., & Smulders, A. (2021). *Vraagstukken en perspectieven voor ict scrm – een initiële verkenning.* Den Haag: TNO. Retrieved from https://www.ncsc.nl/documenten/rapporten/2021/april/28/tno-2021-r10245-vraagstukken-en-perspectieven-voor-ict-scrm-âĂŞ-een-initiele-verkenning

Vigliarolo, B. (2023). *That 3cx supply chain attack keeps getting worse: Other vendors hit.* The Register. Retrieved from https://www.theregister.com/2023/04/24/in_brief_security/ (Acessed on 20.07.2023)

Wang, S. (2017). Knowledge set of attack surface and cybersecurity rating for firms in a supply chain. doi: https://dx.doi.org/10.2139/ssrn.3064533

Warren, M., & Hutchinson, W. (2000). Cyber attacks against supply chain management systems: a short note. *International Journal of Physical Distribution & Logistics Management*, *30*, 960-995.

Webster, J., & Watson, R. T. (2002, 6). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *Vol. 26*, 13-23.

Wieland, A., & Wallenburg, C. M. (2013, 5). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution and Logistics Management*, *43*, 300-320. doi: 10.1108/IJPDLM-08-2012-0243

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, *12*, 4-11. doi: 10.1016/j.ijcip.2015.11.003

Declaration of Academic Integrity

I hereby confirm that the present work is the result of my own independent scholarly work, and that in all cases material from the work of others (in books, articles, essays, dissertations, and on the internet) is acknowledged, and quotations and paraphrases are clearly indicated. No material other than that listed has been used. I have read and understood the Universities regulations and procedures concerning plagiarism.

Jonathan Weiss
2885581

Appendix

Appendix A - Elements of the Conceptual Framework

TABLE A1. Concepts of the conceptual framework derived from the literature review.

Element type	Concept	Author
Structural elements	CSC Infrastructure	Sobb et al. (2020); Creazza et al. (2022); Gani and Fernando (2018); Garvey et al. (2021); Boyens et al. (2022)
	SC Partner Ecosystem	Melnyk et al. (2022); Garvey et al. (2021); Boyens et al. (2020)
Mediating elements	C-SCRM Objectives	Windelberg (2016); Sawik (2022a); Boyes (2015)
	Cybersecurity Investments	Sawik (2022a); Creazza et al. (2022); Deane et al. (2022)
	Mandates	Ludvigsen et al. (2022); Melnyk et al. (2022); Boyens et al. (2020)
	Standards and Frameworks	Schauer et al. (2019); Topping et al. (2021); Shoemaker et al. (2012); Shoemaker and Mead (2013); Shankles et al. (2013); Bartol (2014); Lu et al. (2015); Boyens et al. (2020)
Moderating elements	Collaboration	Sobb et al. (2020); Colicchia et al. (2019); Topping et al. (2021); Nygård and Katsikas (2022); Deane et al. (2022); Cheung et al. (2021); Masip-Bruin et al. (2021); Boyens et al. (2022, 2020); Pandey et al. (2020)
	Organisational Capacity	Colicchia et al. (2019); Deane et al. (2022); Boyens et al. (2020)
	Organisational Agility	Garvey et al. (2021); Fernando et al. (2023)
Main objectives	Cyber Resilience	Colicchia et al. (2019); Creazza et al. (2022); Garvey et al. (2021); Masip-Bruin et al. (2021); Melnyk et al. (2022); Boyes (2015)
	Cyber Robustness	Garvey et al. (2021); Bartol (2014); Windelberg (2016)
	Cyber Assurance	Topping et al. (2021); Hampton et al. (2021); Nygård and Katsikas (2022); Shoemaker et al. (2012); Shankles et al. (2013); Davidson and Shankles (2013); Shoemaker and Mead (2013); Shoemaker and Wilson (2013); Bartol (2014)

Appendix B - Introduction to the Research Interview

Introduction to the study as preparation for the interview about Cyber Supply Chain Risk Management

The problem: Today's business operation relies heavily on the support through products and services from a variety of suppliers. Every piece of supplied hardware, software, cloud or local storage and distribution mechanisms used by an organization to design, manufacture and deliver a product or service can be considered as part of the so-called **cyber supply chain**. However, just like in a physical supply chain, there's a risk that one of these suppliers (or their products and services) might have vulnerabilities or malicious intentions that could compromise the security of the final product or service. The rising complexity of product and service supply chains further limits the visibility and control a firm has into the underlying supplier structure (see figure 1). In the recent years we have seen a substantial rise of supply chain attacks, which usually target smaller suppliers by hijacking their products/ services to attack their customers (e.g. inserting malicious code into signed updates). A recent example is the attack on the VoIP-provider 3CX (read more). The example demonstrates that the security of a company and its products and services, which are eventually passed on to customers, are undeniably linked to the risk posed by the suppliers and their deliveries. In this context, the newly published NIS2 Directive will demand organizations to approach supply chain cybersecurity. The announced Cyber Resilience Act (expected in 2025/2026) will complement it by posing requirements and third-party assessments for digital products.

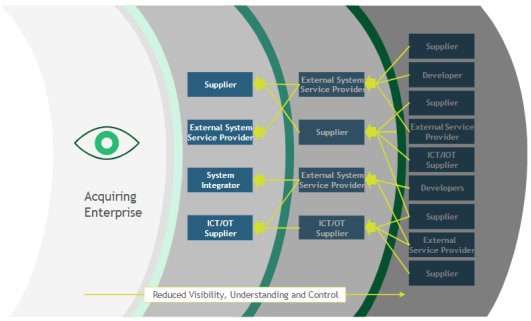

Figure 1: Visibility and control of an enterprise's supply chain (from NIST SP 800-161r1)

Cyber Supply Chain Risk Management aims to identify and mitigate potential cybersecurity risks that can arise from the supply chain of products and services throughout their lifetime, from design to disposal. As a systematic process, it involves the understanding of cyber supply chain risks by evaluating suppliers for their security practices and the security of the components or software they provide, setting security expectations, auditing for compliance and monitoring and improving related cyber supply chain security practices. As a result, companies can reduce the chances of security breaches, data leaks or other cyberattacks that could harm their customers or their own reputation. Further, organizations can improve operational efficiency, assure the quality and reliability of acquired products and services, and establish trust in suppliers and service providers to meet performance requirements.

The accompanying study of the research identified elements internal and external to an organization that have an influence on the development and operation of an organizational-wide cyber supply chain risk management. It is therefore trying to answer how these elements influence the desired outcomes: supply chain robustness, -resilience and -assurance. The interview will therefore touch on familiar concepts from cyber security and supply chain management as well as general deployment of risk management. This will include questions on factors that specify how an organizational cyber supply chain risk management is developed (e.g. use of standards, internal/ external requirements) as well as factors that influence the effectiveness and efficiency of a cyber supply chain risk management program (e.g. threat information sharing or agility). The goal of the interview is to explore the type and significance of the influence, as well as the identification of additional factors. It is important to mention that a deep understanding on each of the sub-discipline just mentioned is not required! The research benefits much more from your professional insights and related expertise.

Appendix C - Informed Consent Form for Participation in Research

Informed Consent Form for Participation in Research

A copy of this form shall be given to the participant

The goal of the study is to identify and evaluate the influence of structural elements and drivers for organizational cyber supply chain risk management. The interview shall take approximately 45 minutes.

By signing this form, I agree to the following:

1. I voluntarily agree to participate in this research study. I declare in a manner obvious to me, to be informed about the nature, method, target of the research. I had the opportunity to ask questions prior to the interview.
2. I understand that I will not benefit directly from participating in this research.
3. I agree to my interview being audio- and video-recorded.
4. I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.
5. I understand that the data obtained from the interviews will be used exclusively for the subsequent master thesis.
6. I understand that a transcript of my interview in which all identifying information has been removed will be retained only for the direct supervisors of the subsequent master thesis.
7. I understand that I can withdraw permission to use data from my interview at any time after the interview, without any specific reason.
8. I understand that I can contact the researcher for further questions at any time during and after the research via j.a.weis@student.utwente.nl

Name Participant	Date	Signature

I wish to receive the transcripts prior to publishing of the study for approval: Yes ☐ | No ☐

I have accurately read out the consent form to the participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

Name Researcher	Date	Signature

Contact information for questions about your rights as a participant

If you have questions about your rights as a research participant, or wish to obtain information, ask questions, or discuss any concerns with this study with someone other than the researcher(s), please contact the Secretary of the Ethics Committee of the EEMCS at the University of Twente by

ethics-comm-eemcs@utwente.nl

UNIVERSITY OF TWENTE.

Appendix D - Interview Guide

Warm Up/ Opening questions:

What thoughts does the introduction raise in you?

What does "supply chain" mean for your role/ organization?

Core/In-depth questions:

1. What are the most important supply chains in your company? (SC Partner Ecosystem)
2. Who are your main suppliers, and what are the major issues with them? (SC Partner Ecosystem)
   a. What about the different kinds of relationships/ dependencies?
      Which peculiarities do you see in the different relationships (e.g., buyer/supplier)?
   b. What about the firms' size of a partner in the supply chain?
      How does the firms' size of a supplier/partner impact a relationship?
   c. What about the level of structural integration/ alignment between partners/ internally?
      How would you describe the effects of structural integration with suppliers?
3. Do you have visibility into your supply chain (beyond tier1)? (SC Visibility)
   a. What is the level of detail?
   b. How do you achieve that?
   c. What are the issues?
4. How flexible is you supplier ecosystem? (SC Flexibility)
   a. Are you able to adapt your relationships with suppliers/ even replace them?
   b. Do you perceive flexibility as important regarding potential cyber risks?
5. How fast are you able to react\respond to uncertainties or changing circumstances in your supply chain (alter/ rearrange relationships or dependencies)? (Agility)
   a. How important do you consider the speed at that the reaction happens?
6. Is the CSC an important issue for you? How would you approach it?
   a. Do you assess/ have information on the attack surface\ risks of used services, products due to a certain technology, architecture etc.?
   b. Do you consider/ assess how exposed to cyberspace your services/ products are (e.g. nr. of ports)?
7. What would you consider the cybersecurity foundations for supply chain cybersecurity? (CS Readiness)
8. Does your organization have set security objectives for managing cyber risks in the supply chain?
   a. What do you consider as necessary CS objectives to manage cyber supply chain risks?
   b. Does one have to extend the classical CIA triad? (CS Objectives)
9. Are you using (together with suppliers) any standards or frameworks to manage cybersecurity risks in the supply chain? Do you see problems in the current landscape, and how to solve them?
10. Do you have any requirements for cybersecurity in your supply chain? From suppliers? How do the suppliers deal with those requirements (reactions/ strategies)? (Mandates)
11. How do you ensure to stay aware of current vulnerabilities and recent changes in your landscape (and of your suppliers/partners)? (Situational awareness)
12. How do you collaborate with your supply chain partners in the context of cybersecurity?
    a. What about (threat) information sharing/ joint knowledge creation?
    b. What about joint decision-making?
    c. What about resource sharing?
13. How do you coordinate your CS investments in the supply chain context? (CS Investments)
14. What are the factors influencing CS investment decisions in a supply chain context?

Wrap-Up/ Closure:

Can you think of anything else you would like to add? Did I miss something?

How do you think about C-SCRM in practice for the future (e.g., under NIS2)?

How do you see yourself involved in that (in your current function/ organisation)?

Appendix E - Results of Open, Axial, and Selective Coding

TABLE A2. Codebook after Open Coding.

Code	Grounded	Code	Grounded
Alternative for Assurance	1	No Collaboration	8
Assurance Standards	10	No Coordinated Investments	5
Barriers for Visibility	5	No Flexibility	4
Benefits of Assurance	1	No Internal Alignment	5
C-SCRM Perspectives	4	No joint-decision making	1
C-SCRM Prerequisites	2	No Supplier Capacity	1
Certification Entities	1	No Visibility	4
Challenges in C-SCRM	13	Organisation Structure	2
Checking Requirements	13	Other	3
CIA as core	1	Perspective of Standards and Frameworks	1
Collaboration Establishing Standards	3	Physical Supply Chain	2
Common Approach for Assurance	2	Posing Requirements	16
Continue investing	1	Problem Awareness	17
Coordinated Investments	8	Problem Complexity	11
CSC Characteristics	4	Problems with Assurance	7
CSC Infrastructure	2	Realizing Objectives	1
Current C-SCRM Efforts	1	Reasons for Collaboration	7
Dealing with Requirements	7	Reasons For Flexibility	2
Demand for External Support	3	Regulation Benefit	1
Develop Standard	2	Regulation Compliance	2
Different Relationships	9	Relationship expectations	1
Ecosystem	4	Relationship Influence	2
Enable Collaboration	4	Relationship Issues	2
Enhancing Visibility	11	Requirements to Supplier Type	2
Establish Own Capabilities	2	Resilience	4
Exit Strategy	5	Responsibility	7
Extending CIA	3	Risk Assessment	3
External Alignment	4	Risk Human Factor	1
Financial Flows	4	Robustness	1
Flexibility Issues	8	Role of Research	1
Flexibility Multi-Vendor Approach	1	Scope of Measures	4
Governance Structures	1	Scope of Requirements	4
Handling incidents	2	Sector Collaboration	4
Heavy Regulated Sector	1	Security Foundations	2
Improve Internal Alignment	4	Small Organizations	3
Improve Visibility	7	Sources Situational Awareness	12
Improving Relationship	7	Supplier Business Criticality	7
Incident-Driven Investment	1	Supplier Criticality	6
Incidents	1	Supplier Issues	4
Increase Flexibility	10	Supplier Technical Criticality	5
Internal Alignment	5	Supply Chain Definition	5
IoT	1	Supply Chain Perspective	11
Issues in coordinated Investments	2	System Lifecycle	1
Mitigation Strategies	12	Transparency	4
Modes of Collaboration	17	Trust	7
Multiple Suppliers Share Task	1	Upcoming Regulation	13
N-Tier Supplier Assessment	2	Using Questionnaires	10
Need for Regulation/ Standard	5	Using Standards as Requirement	7
NIS2 Raises Awareness	2	Using standards/ frameworks for C-SCRM	6
No Agility	1		

TABLE A3. Codebook after Axial Coding.

Code	Grounded	Code	Grounded
Alignment	19	Mitigation Strategies	15
External Alignment	4	Problem Context	55
Improve Internal Alignment	4	C-SCRM Perspectives	4
Internal Alignment	6	Current C-SCRM Efforts	6
No Internal Alignment	5	Problem Awareness	20
C-SCRM Objectives	4	Problem Complexity	6
Extending CIA	4	Supply Chain Definition	5
C-SCRM Prerequisites/ Readiness	5	Supply Chain Perspective	14
Challenges in C-SCRM	13	Relationships	35
Collaboration	46	Different Relationships	10
Enable Collaboration	6	Improving Relationship	7
Modes of Collaboration	18	Relationship Influence	4
No Collaboration	10	Relationship Issues	3
Reasons for Collaboration	7	Transparency	4
Sector Collaboration	5	Trust	7
CS Investments	17	Resilience	4
Coordinated Investments	10	Responsibilities	9
Issues in coordinated Investments	2	SC Cyber Assruance	27
No Coordinated Investments	5	Assurance Standards	11
CSC Infrastructure	26	Common Approach for Assurance	8
Architectural Overview	6	Problems with Assurance	8
Supplier Business Criticality	13	SC Partner Ecosystem	6
Supplier Technical Criticality	8	Situational Awareness	13
Demand for External Support	5	Small Organizations	4
Financial Flows	4	Standards/ Frameworks	15
Flexibility	33	Develop Standard	2
Exit Strategy	5	Using Standards as Requirement	7
Flexibility Issues	8	Using standards/ frameworks for C-SCRM	6
Increase Flexibility	12	Visibility	29
No Flexibility	6	Barriers for Visibility	6
Reasons For Flexibility	2	Enhancing Visibility	12
Mandates	73	Improve Visibility	7
Checking Requirements	13	No Visibility	5
Dealing with Requirements	7		
Need for Regulation	3		
Posing Requirements	18		
Scope of Requirements	5		
Upcoming Regulation	17		
Using Questionnaires	10		

TABLE A4. Codebook after Selective Coding.

Code	Grounded	Code	Grounded
Alignment *[SC Partner Ecosystem]*	28	Mitigation Strategies *[Other]*	14
External Alignment	4	Partner Ecosystem *[SC Partner Ecosystem]*	9
Internal Alignment	12	Problem Context *[Other]*	45
Lack of Internal Alignment	5	C-SCRM Perspectives	4
Responsibilities	10	Problem Awareness	20
C-SCRM Readiness *[Organisational Capacity]*	6	Problem Complexity	6
Collaboration	53	Supply Chain Definition	5
Barriers for Collaboration	4	Supply Chain Perspective	10
Demand for External Support	5	Relationships *[SC Partner Ecosystem]*	34
Enabler for Collaboration	5	Different Relationships	9
Modes of Collaboration	20	Improving Relationship	6
No Collaboration	7	Influence and Power in Relationships	4
Reasons for Collaboration	7	Relationship Issues	4
Sector Collaboration	5	Transparency	4
CS Investments	14	Trust	8
Approch for Coordinated Investments	5	SC Cyber Assruance	27
Issues in coordinated Investments	2	Assurance Practices	10
No Coordinated Investments	7	Need for Common Approach for Assurance	6
CSC Infrastructure	30	Problems with Assurance	12
Architectural Overview	6	SC Cyber Resilience/ Robustness	4
Financial Flows	4	Situational Awareness *[Organisational Capacity]*	13
Supplier Business Criticality	13	Small Organizations *[SC Partner Ecosystem]*	4
Supplier Technical Criticality	8	Standards/ Frameworks	15
Extending CIA *[C-SCRM Objectives]*	4	Develop Standard	2
Flexibility *[Organisational Agility]*	33	Using Standards as Requirement	7
Approaches to Flexibility	19	Using standards/ frameworks for C-SCRM	6
Flexibility Issues	7	State of C-SCRM *[Other]*	21
No Flexibility	7	Challenges in C-SCRM	13
Mandates	61	Current C-SCRM Efforts	8
Approaches to Set Requirements	7	Visibility *[Organisational Capacity]*	30
Checking Requirements	14	Barriers for Visibility	7
Creating Sets of Requirements	6	Enhancing Visibility	16
Dealing with Requirements	10	No Visibility	6
Demanding Certifications	5		
Effects of Upcoming Regulation	17		
Need for Regulation	3		